

70 JA999 240

日 本 国 特 許 庁

PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application:

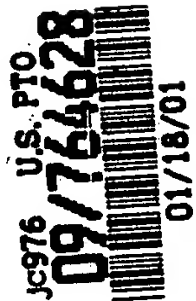
2000年 1月21日

出 願 番 号
Application Number:

特願2000-012520

出 願 人
Applicant(s):

インターナショナル・ビジネス・マシーンズ・コーポレイション

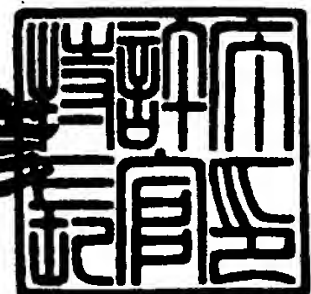


CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年 3月24日

特許庁長官
Commissioner,
Patent Office

近 藤 隆 彦



出証番号 出証特2000-3021162

【書類名】 特許願

【整理番号】 JA999240

【あて先】 特許庁長官 殿

【国際特許分類】 H04N 7/167
H04N 5/225

【発明者】

【住所又は居所】 神奈川県大和市下鶴間 1 6 2 3 番地 1 4 日本アイ・ピー・エム株式会社 東京基礎研究所内

【氏名】 上條 浩一

【発明者】

【住所又は居所】 神奈川県大和市下鶴間 1 6 2 3 番地 1 4 日本アイ・ピー・エム株式会社 東京基礎研究所内

【氏名】 森本 典繁

【発明者】

【住所又は居所】 神奈川県大和市下鶴間 1 6 2 3 番地 1 4 日本アイ・ピー・エム株式会社 東京基礎研究所内

【氏名】 利根川 聡子

【特許出願人】

【識別番号】 390009531

【住所又は居所】 アメリカ合衆国 1 0 5 0 4、ニューヨーク州アーモンク
(番地なし)

【氏名又は名称】 インターナショナル・ビジネス・マシーンズ・コーポレーション

【代理人】

【識別番号】 100086243

【弁理士】

【氏名又は名称】 坂口 博

【選任した代理人】

【識別番号】 100091568

【弁理士】

【氏名又は名称】 市位 嘉宏

【手数料の表示】

【予納台帳番号】 024154

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9706050

【包括委任状番号】 9704733

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 画像処理装置およびその方法

【特許請求の範囲】

【請求項 1】

所定の処理により加わる誤差によって量子化処理後の値が変化しないように画像データの値を変換する変換手段（3 2）と、

画像データに対して前記所定の処理を行う処理手段（3 0 0， 3 0 2）と、

前記所定の処理がなされた画像データを量子化処理する量子化手段（3 0 4）

と

を有する画像処理装置。

【請求項 2】

前記処理手段は、前記画像データを分割し、分割した画像データそれぞれに埋め込みデータを埋め込む埋込処理を行い（5 0）、

前記分割された画像データそれぞれに埋め込まれた埋め込みデータを検出する検出手段（6 0）

をさらに有する請求項 1 に記載の画像処理装置。

【請求項 3】

前記変換手段は、

画像データに含まれる画素それぞれの形式を変換する形式変換手段（3 2 6， 3 3 0）と、

前記量子化処理に用いられる量子化値に基づいて、前記形式が変換された画素データの値を調節処理する調節手段（3 3 2）と

を有し、

前記形式が変換された画素データそれぞれが、前記所定の処理により加わる誤差の値により量子化処理後の値が変化しないようになるまで、前記形式変換処理と、前記調節処理とを繰り返す

請求項 1 に記載の画像処理装置。

【請求項 4】

前記処理手段は、前記画像データに対して埋込データを埋め込む埋込処理を前

記所定の処理として行う

請求項 1 に記載の画像処理装置。

【請求項 5】

前記処理手段は、

所定の鍵情報と前記画像データとに基づいてハッシュ値を計算するハッシュ値計算手段（300）と、

計算の結果として得られた前記ハッシュ値を、前記画像データに埋め込む埋込処理手段（302）と

を有する請求項 4 に記載の画像処理装置。

【請求項 6】

前記画像データに埋め込まれた埋込データを検出する検出手段（30）

をさらに有する請求項 4 または 5 に記載の画像処理装置。

【請求項 7】

前記量子化された画像データを逆量子化する逆量子化手段（422）と、

前記逆量子化された画像データに埋め込まれたハッシュ値を抽出する抽出手段（400）と、

前記画像データと、前記ハッシュ値の計算に用いられた鍵情報とに基づいて、ハッシュ値を計算する計算手段（402）と、

前記抽出されたハッシュ値と前記計算されたハッシュ値とに基づいて、前記量子化された画像データに改ざんが加えられたか否かを検出する改ざん検出手段（404）と

を有する請求項 5 に記載の画像処理装置。

【請求項 8】

所定の処理により加わる誤差によって量子化処理後の値が変化しないように画像データの値を変換し、

画像データに対して前記所定の処理を行い、

前記所定の処理がなされた画像データを量子化処理する

画像処理方法。

【請求項 9】

所定の処理により加わる誤差によって量子化処理後の値が変化しないように画像データの値を変換する変換ステップと、

画像データに対して前記所定の処理を行う処理ステップと、

前記所定の処理がなされた画像データを量子化処理する量子化ステップと

をコンピュータに実行させるプログラムを記録した記録媒体。

【請求項 1 0】

前記処理ステップは、前記画像データを分割し、分割した画像データそれぞれに埋め込みデータを埋め込む埋込処理を行い、

前記分割された画像データそれぞれに埋め込まれた埋め込みデータを検出する検出ステップ

をさらに有する請求項 9 に記載の記録媒体。

【請求項 1 1】

前記変換ステップは、

画像データに含まれる画素それぞれの形式を変換する形式変換ステップと、

前記量子化処理に用いられる量子化値に基づいて、前記形式が変換された画素データの値を調節処理する調節ステップと

を有し、

前記形式が変換された画素データそれぞれが、前記所定の処理により加わる誤差の値により量子化処理後の値が変化しないようになるまで、前記形式変換処理と、前記調節処理とを繰り返す

請求項 9 に記載の記録媒体。

【請求項 1 2】

前記処理ステップは、前記画像データに対して埋込データを埋め込む埋込処理を前記所定の処理として行う

請求項 9 に記載の記録媒体。

【請求項 1 3】

前記処理ステップは、

所定の鍵情報と前記画像データとに基づいてハッシュ値を計算するハッシュ値計算ステップと、

計算の結果として得られた前記ハッシュ値を、前記画像データに埋め込む埋込処理ステップと

を有する請求項 1 2 に記載の記録媒体。

【請求項 1 4】

前記画像データに埋め込まれた埋込データを検出する検出ステップ

をさらに有する請求項 1 2 または 1 3 に記載の記録媒体。

【請求項 1 5】

前記量子化された画像データを逆量子化する逆量子化ステップと、

前記逆量子化された画像データに埋め込まれたハッシュ値を抽出する抽出ステップと、

前記画像データと、前記ハッシュ値の計算に用いられた鍵情報とに基づいて、ハッシュ値を計算する計算ステップと、

前記抽出されたハッシュ値と前記計算されたハッシュ値とに基づいて、前記量子化された画像データに改ざんが加えられたか否かを検出する改ざん検出ステップと

を有する請求項 1 3 に記載の記録媒体。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、著作権情報などの認証情報（埋め込みデータ）を埋め込んだ画像データ等を、圧縮のために量子化しても、埋め込まれた認証データが失われないようにした画像処理装置およびその方法に関する。

【0 0 0 2】

【従来の技術】

例えば、国際公開 W O 9 7 / 4 9 2 3 5 号公報（文献 1）は、ピクセル・ブロック・コーディング（Pixel Block Coding ; P B C）により、画像データ等のコンテンツデータに著作権情報など（以下、一般的に認証情報あるいは埋め込みデータ等とも記す）を、視覚的に感知できないように埋め込む方式（以下、このようにコンテンツデータに感知できないように認証方法を埋め込む方式を「エレクトロニクス」

トロニックウォーターマーキング方式」とも記す)を開示する。

【0003】

また、国際公開WO98/116928号公報(文献2)は、文献1等を開示されたエレクトロニックウォーターマーキング方式を応用して、画像データの改変を禁止し、著作物を有効に保護する方法を開示する。

また、特開平10-164549号公報(文献3)は、文献1等を開示されたエレクトロニックウォーターマーキング方式を改良し、画像データに認証情報を一体不可分に埋め込むことにより、画像データの改変を検出する方法を開示する。

【0004】

また、これらの文献の他、特開平09-151747号公報、特開平10-83310号公報、特開平10-106149号公報、特開平10-161933号公報、特開平10-164349号公報、特開平10-285562号公報、特開平10-334272号公報、特開平10-240626号公報、特開平10-240129号公報(文献4~12)等も、エレクトロニックウォーターマーキング方式に関する発明を開示する。

【0005】

しかしながら、これらの文献に開示された方式は、認証情報を埋め込んだ後の画像データの圧縮符号化を十分に考慮していなかった。つまり、これらの方式により埋め込まれた認証情報が量子化値より少ない場合には、埋め込まれた画像データが量子化の結果、消失してしまう可能性がある。

【0006】

【発明が解決しようとする課題】

本発明は、上述した従来技術の問題点に鑑みてなされたものであり、圧縮符号化に適した画像処理装置およびその方法を提供することを目的とする。

特定的には、本発明は、認証情報を埋め込んだ後に量子化処理をしても、埋め込まれた認証情報が失われることがない画像処理装置およびその方法を提供することを目的とする。

【0007】

【課題を達成するための手段】

上記目的を達成するために、本発明にかかる画像処理装置は、所定の処理により加わる誤差によって量子化処理後の値が変化しないように画像データの値を変換する変換手段と、画像データに対して前記所定の処理を行う処理手段と、前記所定の処理がなされた画像データを量子化処理する量子化手段とを有する。

【0008】

好適には、前記処理手段は、前記画像データを分割し、分割した画像データそれぞれに埋め込みデータを埋め込む埋込処理を行い、前記分割された画像データそれぞれに埋め込まれた埋め込みデータを検出する検出手段をさらに有する。

【0009】

好適には、前記変換手段は、画像データに含まれる画素それぞれの形式を変換する形式変換手段と、前記量子化処理に用いられる量子化値に基づいて、前記形式が変換された画素データの値を調節処理する調節手段とを有し、前記形式が変換された画素データそれぞれが、前記所定の処理により加わる誤差の値により量子化処理後の値が変化しないようになるまで、前記形式変換処理と、前記調節処理とを繰り返す。

【0010】

好適には、前記処理手段は、前記画像データに対して埋込データを埋め込む埋込処理を前記所定の処理として行う。

【0011】

好適には、前記処理手段は、所定の鍵情報と前記画像データとに基づいてハッシュ値を計算するハッシュ値計算手段と、計算の結果として得られた前記ハッシュ値を、前記画像データに埋め込む埋込処理手段とを有する。

【0012】

好適には、前記画像データに埋め込まれた埋込データを検出する検出手段をさらに有する。

【0013】

好適には、前記量子化された画像データを逆量子化する逆量子化手段と、前記逆量子化された画像データに埋め込まれたハッシュ値を抽出する抽出手段と、前

記画像データと、前記ハッシュ値の計算に用いられた鍵情報とに基づいて、ハッシュ値を計算する計算手段と、前記抽出されたハッシュ値と前記計算されたハッシュ値とに基づいて、前記量子化された画像データに改ざんが加えられたか否かを検出する改ざん検出手段とを有する。

【 0 0 1 4 】

また、本発明にかかる画像処理方法は、所定の処理により加わる誤差によって量子化処理後の値が変化しないように画像データの値を変換し、画像データに対して前記所定の処理を行い、前記所定の処理がなされた画像データを量子化処理する。

【 0 0 1 5 】

また、本発明にかかる記録媒体は、所定の処理により加わる誤差によって量子化処理後の値が変化しないように画像データの値を変換する変換ステップと、画像データに対して前記所定の処理を行う処理ステップと、前記所定の処理がなされた画像データを量子化処理する量子化ステップとをコンピュータに実行させるプログラムを記録する。

【 0 0 1 6 】

【発明の実施の形態】

〔第 1 実施形態〕

以下、本発明の第 1 実施形態を説明する。

【 0 0 1 7 】

〔改変判定装置 1〕

図 1 は、本発明にかかる画像処理方法を実現する画像処理装置 1 の構成を示す図である。

図 1 に示すように、画像処理装置 1 は、C R T 表示装置あるいは液晶表示装置等の表示装置 1 0 0、キーボードおよびマウス等を含む入力装置 1 0 2、デジタルカメラインターフェース I F（カメラ I F）1 0 4、メモリカードインターフェース（メモリカード I F）1 0 6、M O 装置および C D 装置等の記憶装置 1 0 8、および、メモリ 1 1 2 およびマイクロプロセッサ（C P U）1 1 4 等を含むコンピュータ本体（P C 本体）1 1 0 から構成され、必要に応じて、さらに通

信装置 1 1 6 が付加される。

つまり、画像処理装置 1 は、一般的なコンピュータに、カメラ I F 1 0 4 およびメモ리카ード I F 1 0 6 を付加した構成を採る。

【 0 0 1 8 】

画像処理装置 1 は、これらの構成部分により、デジタルカメラ 1 4 0 が撮影した画像データ（J P E G、B M PあるいはY U Vなど形式を問わない）を、カメラ I F 1 0 4 を介して受け入れる。あるいは、画像処理装置 1 は、デジタルカメラ 1 4 0 がメモ리카ード 1 4 2 に記録した画像データを、メモ리카ード I F 1 0 6 を介して受け入れる。

【 0 0 1 9 】

さらに、画像処理装置 1 は、光磁気ディスク（M O）あるいはコンパクトディスク（C D）等の記録媒体 1 2 0 に記録されて記憶装置 1 0 8 に供給される埋込・検出プログラム 2（図 2 等を参照して後述する）を、メモリ 1 1 2 にロードして実行し、受け入れた画像データに対して、量子化処理しても失われることがないように電子透かし（埋め込みデータ）の埋め込み処理を行う。

【 0 0 2 0 】

また、画像処理装置 1 は、埋込・検出プログラム 2 を実行し、画像データに埋め込まれた電子透かしを検出し、画像データに対して改ざんが加えられたか否か等を判定する。

【 0 0 2 1 】

[埋込・検出プログラム 2]

まず、埋込・検出プログラム 2 の構成および動作を説明する。

図 2 は、図 1 に示した画像処理装置 1 が実行し、本発明にかかる画像処理方法を実現する埋込・検出プログラム 2 の構成を示す図である。

図 2 に示すように、埋込・検出プログラム 2 は、O S 8 0、埋込・抽出部 3、鍵情報データベース（D B） 2 2 および画像データベース（D B） 2 4 から構成される。

埋込・抽出部 3 は、埋込パラメータ D B 2 0、制御部 2 6、埋込部 3 0 および抽出部 4 0 から構成される。

【 0 0 2 2 】

[O S 8 0]

O S 8 0 は、例えば、O S / 2 (I B M 社) あるいはウィンドウズ (マイクロソフト社) 等のオペレーティングシステムソフトウェアであって、埋込・検出プログラム 2 の各構成部分の実行制御を行う。

【 0 0 2 3 】

[制御部 2 6]

埋込・抽出部 3 の制御部 2 6 は、例えば、表示装置 1 0 0 に操作用の G U I 画像 (図示せず) を表示し、表示された G U I 画像に対するユーザの操作を受け入れ、必要に応じて、受け入れた操作を示す操作データを、埋込・検出プログラム 2 の各構成部分に供給する。

また、制御部 2 6 は、受け入れたユーザの操作に応じて、埋込・検出プログラム 2 の各構成部分の動作を制御する。

【 0 0 2 4 】

[画像 D B 2 4]

画像 D B 2 4 は、埋込部 3 0 が電子透かしを埋め込んだ圧縮画像データ (J P E G データ) を記憶装置 1 0 8 に挿入された記録媒体 1 2 0、あるいは、メモ리카ード I F 1 0 6 に挿入されたメモ리카ード 1 4 2 に記憶・管理し、記憶・管理した画像データを読み出して抽出部 4 0 に対して出力する。

【 0 0 2 5 】

[鍵情報 D B 2 2]

鍵情報 D B 2 2 は、画像 D B 2 2 が管理する J P E G データと、埋込部 3 0 が、この J P E G データへ電子透かしを埋め込む際に、乱数を発生させるために用いる鍵 (例えば 6 4 ビットの数値) とを対応付けた鍵情報を記憶装置 1 0 8 等に記憶・管理し、記憶・管理した鍵情報を読み出して埋込部 3 0 および抽出部 4 0 に対して出力する。

【 0 0 2 6 】

[埋込パラメータ D B 2 0]

埋込パラメータ D B 2 0 は、電子透かしの埋め込みに用いるパラメータを記憶

・管理し、埋込部 3 0 に対して出力する。

【 0 0 2 7 】

〔埋込部 3 0〕

図 3 は、図 2 に示した埋込部 3 0 の構成を示す図である。

図 4 は、注目 D C T 係数を示す図である。

図 3 に示すように、埋込部 3 0 は、埋込前処理部 3 2、ハッシュ (H a s h) 値計算部 3 0 0、ハッシュ値埋込部 3 0 2 および出力フォーマット変換部 3 0 4 から構成される。

埋込部 3 0 は、これらの構成部分により、まず、各種 (J P E G、R G B (ビットマップ (B M P)) および輝度・色差 (Y U V) 等) の形式の画像データから、予め定められたハッシュ関数とキーとを用いて、注目する D C T (図 4) 係数のハッシュ値を計算する。

【 0 0 2 8 】

さらに、埋込部 3 0 は、計算の結果として得たハッシュ値を、画像データ自体に対して電子透かしの手法を用いて埋め込む、あるいは、画像データのヘッダ部分に埋め込む等の方法により、画像データに付加する。

なお、埋込部 3 0 を画像データの Y, U, V 各成分から得られた D C T 係数に対して、電子透かしの手法を用いてハッシュ値を埋め込むように構成すること、Y, C r, C b 各成分から得られた D C T 係数に対してハッシュ値を埋め込むように構成することも可能であるが、説明の明確化のために、以下、埋込部 3 0 が、計算して得たハッシュ値を、画像データの Y, U, V 各成分から得られた D C T 係数に対して埋め込む場合を具体例とする。

【 0 0 2 9 】

〔埋込前処理 3 2〕

図 5 は、図 3 に示した埋込前処理部 3 2 の構成を示す図である。

また、図 5 に示すように、埋込パラメータ D B 2 0 (図 2) の埋込前処理 3 2 は、フォーマット認識部 3 2 0、逆量子化部 (Q^{-1}) 3 2 2、量子化値計算部 3 2 4、J P E G' / B M P 変換部 3 2 6、Y U V / B M P 変換部 3 2 8、B M P / J P E G' 変換部 3 3 0 および D C T 係数調整部 3 3 2 から構成される。

【 0 0 3 0 】

埋込部 3 0 は、これらの構成部分により、D C T 変換してハッシュ値を埋め込んで電子透かしを埋め込み、さらに、圧縮符号化して J P E G 形式の圧縮画像データ（J P E G データ）とした場合であっても、埋め込んだハッシュ値が失われない状態（安定状態）になるように、画像データ（B M P データ）に対して埋込前処理を行う。

【 0 0 3 1 】

[フォーマット認識部 3 2 0]

埋込前処理 3 2 において、フォーマット認識部 3 2 0 は、入力された各種形式の画像データ（J P E G データ、B M P データ、Y U V 形式の画像データ（Y U V データ）等）のデータフォーマットを識別し、入力された画像データがいずれの形式であるかを判断し、J P E G データが入力された場合には、入力された J P E G データを復号部 3 2 2 に対して出力し、B M P データが入力された場合には、入力された B M P データを B M P / J P E G ' 変換部 3 3 0 に対して出力し、Y U V データが入力された場合には、入力された Y U V データを Y U V / B M P 変換部 3 2 8 に対して出力する。

【 0 0 3 2 】

さらに、フォーマット認識部 3 2 0 は、B M P データにおいてハッシュ値を埋め込む領域を、例えば 16×16 画素構成の M C U 単位で指定する領域指定データ A を受け、領域指定データ A が示す M C U それぞれに含まれる D C T 係数が安定状態であるか否かを示す M C U テーブル T（T [X] [Y]、例えば、B M P データが 720×480 画素構成である場合には $X = 45$ 、 $Y = 30$ ）を作成する。

【 0 0 3 3 】

なお、領域指定データ A により指定される領域は、J P E G ' / B M P 変換部 3 2 6 および Y U V / B M P 変換部 3 2 8 による変換処理の対象とはならない。

画質に与える影響を最小にすることができるという意味で、領域指定データ A を、画面の端の領域を指定するように作成すると、そうでない場合に比べてより好適である。

フォーマット認識部 3 2 0 は、作成したMCUテーブルTを、J P E G データ、BMP データおよびY U V データそれぞれに付して、復号部 3 2 2、BMP / J P E G' 変換部 3 3 0 およびY U V / BMP 変換部 3 2 8 にそれぞれに対して出力する。

【 0 0 3 4 】

上述のように、MCUテーブルTは、例えば4 5 × 3 0 のマトリクス形式で表され、MCUテーブルTの各要素T [X] [Y] それぞれは、例えば、対応するMCUのDCT係数データが安定状態である場合には値1、安定でない場合には値0を採る。

フォーマット認識部 3 2 0 は、下式 1 に示すように、MCUテーブルTの初期値として、領域指定データAが示すMCUに対応するMCUテーブルTの要素T [X] [Y] の値を1とし、これら以外のMCUテーブルの要素T [X] [Y] の値を0とする。

【 0 0 3 5 】

【数 1】

$$\begin{aligned} T [X] [Y] &= 1 && : (X, Y) \in A \text{ の場合} \\ &= 0 && : (X, Y) \in A \text{ 以外の場合} \end{aligned} \quad (1)$$

【 0 0 3 6 】

【復号部 3 2 2】

J P E G データは、DCT係数に対して量子化処理およびハフマン (Huffman) 符号化処理を施すことにより生成される。復号部 3 2 2 は、まず、フォーマット認識部 3 2 0 から入力されたJ P E G データをハフマン復号する。

また、復号部 3 2 2 は、復号したJ P E G データのY, U, V各成分からそれらの量子化値q [k] を計算し、埋込量子化値計算部 3 2 4 に対して出力する。

また、復号部 3 2 2 は、計算の結果として得た量子化値q [k] それぞれを用いて、ハフマン復号したJ P E G データのY, U, V各成分を逆量子化して、Y, U, V各成分のDCT係数J P E G' を生成し、MCUテーブルTと対応づけてJ P E G' / BMP 変換部 3 2 6 に対して出力する。

【 0 0 3 7 】

[YUV/BMP変換部328]

YUV/BMP変換部328は、YUVデータを、下式2に示すようにBMPデータ(RGB)に変換し、MCUテーブルTと対応付けてBMP/JPEG'変換部330に対して出力する。

なお、YUV/BMP変換部328によりYUVデータをBMPデータに変換する理由は、YUVデータのY, U, V各成分が、オーバーフローあるいはアンダーフローを起こしていなくても($0 \leq Y < 256$, $-128 \leq U, V < 128$)、BMPデータに変換した場合に、BMPデータのR, G, B各成分にオーバーフローあるいはアンダーフローが生じる場合があるので、このような場合においても、最終的に得られるDCT係数を安定状態とすることができるようにするためである。

【0038】

【数2】

$$\begin{aligned} R &= (\text{int})(Y + V \cdot 1.4020) \\ G &= (\text{int})(Y - U \cdot 0.3441 - V \cdot 0.7139) \\ B &= (\text{int})(Y + U \cdot 1.7718 - V \cdot 0.0012) \end{aligned} \quad (2)$$

但し、

$$R = R > 255 ? 255 : R < 0 ? 0 : R$$

$$G = G > 255 ? 255 : G < 0 ? 0 : G$$

$$B = B > 255 ? 255 : B < 0 ? 0 : B$$

ここで、 $A = B ? C : D$ は、C codeのものと同じで、

$A = C$ (if B is TRUE)

$A = D$ (if B is NOT TRUE)

である。

【0039】

[JPEG'/BMP変換部326]

JPEG'/BMP変換部326は、復号部322およびDCT係数調整部332から入力されるDCT係数JPEG'の内、領域指定データAが示す領域以外のMCUのY, U, V成分それぞれのDCT係数を逆DCT(IDCT)処理

する。

JPEG' / BMP変換部326は、さらに、IDCT処理の結果として選ばれたY, U, V成分を、YUV / BMP変換部328と同様に上記式2に従ってBMPデータに変換し、MCUテーブルTと対応づけてBMP / JPEG' 変換部330に対して出力する。

【0040】

[BMP / JPEG' 変換部330]

BMP / JPEG' 変換部330は、JPEG' / BMP変換部326、フォーマット認識部320またはYUV / BMP変換部328から入力されるBMPデータの内、同じくこれらから入力されるMCUテーブルTの値0の要素T[X][Y] (T[X][Y] = 0) に対応するMCUに含まれるBMPデータのR, G, B成分それぞれを、下式3に示すように、Y, U, V各成分に変換し、さらに、変換の結果として選ばれたY, U, V各成分を、8×8構成のDCTブロックごとにDCT処理してDCT係数JPEG' を生成する。

つまり、BMP / JPEG' 変換部330は、入力されるBMPデータの内、まだ安定状態になっていないBMPデータをDCT係数JPEG' に変換する。

BMP / JPEG' 変換部330は、変換処理の結果として得られたDCT係数JPEG' を、MCUテーブルTと対応づけてDCT係数調整部332に対して出力する。

【0041】

【数3】

$$\begin{aligned} Y &= R*0.2990 + G*0.5870 + B*0.1140 \\ U &= -R*0.1684 - G*0.3316 + B*0.5000 \\ V &= R*0.5000 - G*0.4187 - B*0.0813 \end{aligned} \quad (3)$$

【0042】

[埋込量子化値計算部324]

埋込量子化値計算部324は、領域指定データAにより示されるDCT係数（注目DCT係数）dct_Coeffiの埋込量子化値q_emb[k]を算出する。

さらに埋込量子化値計算部 3 2 4 の処理を詳細に説明する。

埋込量子化値計算部 3 2 4 は、注目 DCT 係数 dct_coeff_i およびデコード最大計算誤差 δ を、埋込パラメータ DB 2 0 (図 2) から受ける。

【 0 0 4 3 】

[注目 DCT 係数 dct_coeff_i]

ここでは、注目 DCT 係数 dct_coeff_i を詳細に説明する。

注目 DCT 係数 dct_coeff_i は、電子透かしの埋め込みに用いる 8×8 画素構成の DCT ブロックに含まれる 1 つ以上の DCT 係数であり、Y, U, V 成分のいずれの DCT 係数であってもよいが、以下、説明の明確化のために、注目 DCT 係数 dct_coeff_i として Y 成分の DCT 係数の内の直流成分 $dct_coeff_i(0, 0)$ を用い、ハッシュ値の埋め込みのために、同じく Y 成分の DCT 係数の内の $(1, 1)$, $(1, 2)$, $(2, 1)$, $(2, 2)$ を利用する場合を具体例とする。

【 0 0 4 4 】

[デコード最大計算誤差 δ]

ここでは、デコード最大計算誤差 δ を詳細に説明する。

また、ハッシュ値を埋め込んだ J P E G データを伸長復号処理するデコードが違う場合には、システム間で I D C T 処理の結果に誤差が生じる可能性がある。デコード最大計算誤差 δ は、埋め込み量子化値: システム(decoder)の違いから生じる I D C T 処理の誤差の 2 倍の値に設定される。

なお、I D C T 処理の誤差は、ほとんどの場合、2 以下である。従って、デコード最大計算誤差 δ の設定値は 4 以上あれば充分である。以下、デコード最大計算誤差 δ の値を、十分に大きい 1 2 に設定する場合を具体例として説明する。

【 0 0 4 5 】

埋込量子化値計算部 3 2 4 は、埋込前処理 3 2 に入力された画像データが J P E G データである場合には、復号部 3 2 2 から入力された量子化値 $q[k]$ を、J P E G データでない場合には、例えば、入力装置 1 0 2 を介してユーザが入力する量子化値 $q[k]$ を用いて以下の処理を行う。

なお、埋込量子化値計算部 3 2 4 は、例えば、埋込前処理 3 2 に入力された画

像データが J P E G データでなく、しかも、入力装置 1 0 2 から量子化値 $q[k]$ の入力がない場合には、量子化値 $q[k]$ の全ての要素の値をデコーダ最大計算誤差 δ に設定する ($q[k] = \delta$)。

【 0 0 4 6 】

次に、埋込量子化値計算部 3 2 4 は、領域指定データ A が示す注目 D C T 係数 $d c t_c o e f f i$ それぞれに対応する埋込量子化値 $q_e m b[k]$ ($k \in \{d c t_c o e f f i\}$) を、下式 4 に示すように計算する。

なお、埋込量子化値 $q_e m b[k]$ は、ハッシュ値を埋め込んだ D C T 係数を量子化処理するために用いられる量子化値であって、量子化値 $q[k]$ の整数倍の値を採る。

【 0 0 4 7 】

【数 4】

$$q_emb[k] = (\text{int}((\delta - 1)/q[k] + 1) * q[k]) \quad (4)$$

【 0 0 4 8 】

なお、量子化値 $q[k]$ がデコーダ最大計算誤差 δ よりも大きい場合 ($q[k] \geq \delta$)、埋込量子化値 $q_e m b[k]$ と量子化値 $q[k]$ とは一致する ($q_e m b[k] = q[k]$)。

また、埋込前処理 3 2 に J P E G データが入力される場合、量子化値 $q[k]$ の変更は不要である。

【 0 0 4 9 】

【 D C T 係数調整部 3 3 2 】

D C T 係数調整部 3 3 2 は、J P E G' / B M P 変換部 3 2 6、B M P / J P E G' 変換部 3 3 0 および D C T 係数調整部 3 3 2 により構成されるループ処理を制御し、このループ処理を所定の回数 (例えば 5 回) 繰り返して、B M P / J P E G' 変換部 3 3 0 から入力された注目 D C T 係数 $d c t_c o e f f i$ が、埋込量子化値 $q_e m b[k]$ の整数倍に近い値をとるように、つまり、注目 D C T 係数 $d c t_c o e f f i$ が安定状態になるようにそれらの値を調整する。

【 0 0 5 0 】

以下、さらに D C T 係数調整部 3 3 2 の処理を詳細に説明する。

DCT係数調整部332は、埋込パラメータDB20（図2）から安定化閾値 Δ を受ける。

安定化閾値 Δ は、注目DCT係数 dct_coeff_i が、埋込量子化値 $q_emb[k]$ の整数倍に近い値になっているか否かを判断するために用いられる閾値であって、例えばデコーダ最大計算誤差 δ よりも小さい値、例えば1程度の値に設定される（ $\delta > \Delta = 1.0$ ）。

【0051】

DCT係数調整部332は、次に、領域指定データAにより示されるMCUのDCTブロックそれぞれに含まれる各DCT係数が、下式5を満たしているか否かを判断する。

DCT係数調整部332は、判断対象のDCTブロックに含まれるDCT係数のすべてが下式5を満たしている場合には、このDCTブロックに対応するMCUテーブルTの要素T[X][Y]の値を安定状態を示す1とし（T[X][Y] = 1）、これ以外の場合には0とする（T[X][Y] = 0）。

【0052】

【数5】

$$|c[k] - coeff_emb[k] * q_emb[k]| < \Delta / 2 \quad (5)$$

【0053】

DCT係数調整部332は、全てのMCUの全てのDCTブロックに含まれるDCT係数が式5を満たし、安定状態になっている場合には、注目DCT係数 dct_coeff_i およびその他のDCT係数を画像DB24（図2）に対して出力し、安定状態になっていない場合には、安定状態になっていないDCT係数が安定状態になるように調節する。

なお、DCT係数調整部332は、 $coeff_emb[k]$ を、領域指定データAが示す注目DCT係数 dct_coeff_i として、それ以外のDCT係数は、量子化処理した値（ $coeff_i[k] = c[k] / q[k]$ ）を、画像DB24（図2）に対して出力する。

【0054】

〔DCT係数の安定化〕

ここでは、DCT係数調整部332がDCT係数を安定状態にする処理（安定化処理）を詳細に説明する。

DCT係数調整部332は、値が0のMCUテーブルTの要素T[X][Y]に対応するMCUのDCT係数を、下式6に示すように変換する。

【0055】

【数6】

$c[k] = \text{coeff_emb}[k] * q_emb[k] :$

if $k \in \{\text{dct_coeffi}\}$

$c[k] = (\text{int})(c[k] > 0 ? c[k] / q[k] + \alpha : c[k] < 0 ? c[k] / q[k] - \alpha : 0) * q[k]$

otherwise

但し、

$\text{coeff_emb}[k] = (\text{int})(c[k] > 0 ? c[k] / q_emb[k] + \alpha : c[k] < 0 ? c[k] / q_emb[k] - \alpha : 0)$ (6)

【0056】

式6において、 α は0～0.5の間の値を採る数値であって（ $0 \leq \alpha \leq 0.5$ ）、 α の値を大きくすると、安定化処理が再生画像に与える変化を小さくすることができる。しかしながら、変換後の $\text{coeff}[k]$ の値の絶対値は常に大きくなり、安定状態にした後のDCT係数を変換して得られるBMPデータのR、G、B成分の値に近づくので、BMPデータのR、G、B成分の値にオーバーフロー・アンダーフローが生じやすい。

一方、 α を小さくすると、変換後の $\text{coeff}[k]$ の値の絶対値は常に小さくなり、安定状態にした後のDCT係数を変換して得られるBMPデータのR、G、B成分それぞれの値は128に近づくので、BMPデータのR、G、B成分の値にオーバーフロー・アンダーフローが生じにくい。

【0057】

このような α の性質を考慮し、安定化処理が再生画像に与える影響を極力少なくし、かつ、安定化したDCT係数を変換して得られるBMPデータにオーバーフロー・アンダーフローが生じないようにするために、DCT係数調整部332は、JPEG' / BMP変換部326、BMP / JPEG' 変換部330および

DCT係数調整部 3 3 2 によるループ処理を 1 回行うごとに、 α の値を減らしてゆくようにする。

【 0 0 5 8 】

例えば、J P E G ' / B M P 変換部 3 2 6、B M P / J P E G ' 変換部 3 3 0 および D C T 係数調整部 3 3 2 によるループ処理の回数を `loopcount` とすると、D C T 係数調整部 3 3 2 は、下式 7 に示すように、ループ処理の回数に応じて α の値を少なくする。

【 0 0 5 9 】

【数 7】

$$\alpha = \begin{cases} 0.5\text{loopcount}/10 & (\text{loopcount} < 5) \\ 0 & (\text{loopcount} \geq 5) \end{cases} \quad (7)$$

【 0 0 6 0 】

D C T 係数調整部 3 3 2 は、上述した調整を、値が 0 の M C U テーブル T の要素 T [X] [Y] に対応する M C U に含まれる D C T ブロック全ての D C T 係数に対して行い、J P E G ' / B M P 変換部 3 2 6 に対して出力する。

【 0 0 6 1 】

なお、ごくまれに、J P E G ' / B M P 変換部 3 2 6 における処理でオーバーフロー・アンダーフローが生じていて、ループ処理を 5 回繰り返した後でも、式 5 の条件を満たすことがない D C T 係数が存在することがある。

このような場合に対応するために、D C T 係数調整部 3 3 2 は、ループ処理を 5 回繰り返した後は、さらに、D C T 係数の値が式 5 の条件を満たすようになるまでループ処理を 1 回ずつ追加して行い、ループ処理を 1 回追加するたびに、`coeff_emb[k]` の絶対値を 1 (但し、何らかの制約がある場合、その制約を満たす 1 以上の最小数) ずつ減らす。

このように、ループ処理を追加し、ループ処理 1 回ごとに `coeff_emb[k]` の絶対値を 1 (但し、何らかの制約がある場合、その制約を満たす 1 以上の最小数) ずつ減らすことにより、D C T 係数調整部 3 3 2 は、画像の変化を極力少なくしつつ、ループ処理を有限回数に抑える。

【 0 0 6 2 】

以上説明した埋込前処理 3 2 の処理により、図 6 (A) に示すように分布していた注目 DCT 係数 dct_coeff_i の値は、図 6 (B) に示すように、埋込量子化値 $q_emb[k]$ の整数倍に近い値を採るようになり、埋込量子化値 $q_emb[k]$ の整数倍を中心とする広がり σ ($\sigma < \delta$) の範囲内に分布するようになる。

【 0 0 6 3 】

[ハッシュ値計算部 3 0 0]

再び図 3 を参照する。

以上説明した埋込前処理 3 2 (図 3, 4) の処理により、 $\{dec_coeff_i\}$ の全ての DCT 係数が埋め込みの量子化値 $q_emb[k]$ の整数倍の近傍に来て安定化している。即ち、上述した式 5 を満たしている。問題は、埋込前処理 3 2 の出力から得られる JPEG データを、JPEG' / BMP 変換部 3 2 6 (図 5) 以外 BMP エンコーダにより処理して式 5 に示した性質が保てるか否かである。

例えば、埋込前処理 3 2 (図 3, 4) の出力データを $input_bmp$ 、え 4 4 以外のエンコーダで作られる BMP データを $input2_bmp$ とすると、これらの違いは、JPEG データを iDCT し、さらに YUV データに変換し、これを BMP データに変換する処理における計算の誤差であり、この誤差のために、2 つの $input_bmp$ と $input2_bmp$ とが、下式 8 に示すように、量子化値を跨いでしまう可能性が高い。即ち、 $input_bmp$ から導かれた DCT 係数 $c2[k]$ が、下式 8 を満たす可能性は小さい。

【 0 0 6 4 】

【数 8】

$$err[k] = |c2[k] - coeff_emb[k] * q_emb[k]| \geq q_emb[k] / 2 \quad (>= \delta / 2) \quad (8)$$

【 0 0 6 5 】

例えば、ある BMP エンコーダで iDCT 処理結果 (iDCT データ) あるいは YUV データを BMP データに変換する処理を小数点第 1 位まで用いて計算する際に、iDCT データの計算誤差が最悪 0.05 あり、iDCT 処理で、係数 1 つにつき 64 回の加算または減算を行うとすると、計算誤差は最悪 3.35 (

$= 0.05 \times 63 + 3$) となるが、上述したように、最大誤差 δ を 12 より大きい値にとれば、上述した式 8 を満たすことはない。

【0066】

逆に、i D C T 等の計算で少数第 1 位以上の誤差があるようなシステムは、誤差が大きすぎで、単なる変換だけで画像が大きく変化してしまい、使用に耐えないシステムと言える。多数のシステムを調べると、最悪で $\text{err}[k]=3.0$ 程度である。

よって、全ての $\{\text{d c t_c o e f f i}\}$ に対して全ての $\text{q_e m b}[k]$ による量子化値 $\text{c o e f f_e m b}[k]$ は、J P E G データを B M P データに変換する処理に耐えられることになる。そのため、 $\text{c o e f f_e m b}[k]$ のハッシュ値を取り、その結果を J P E G データのヘッダ部分に書き込むか、画像自体に電子透かしで埋めておけば良い。

【0067】

埋め込みに使われる領域 A を除き、鍵 DB からえられる、埋め込み者、検出者で共通の鍵 K を使い、ハッシュ値 D C T_h a s h を、下式 9 に示すように計算する。

【0068】

【数 9】

$$\text{DCT_hash} = \text{hash}(K, \text{coeff_emb}[k]) \quad (9)$$

【0069】

なお、式 9 における $\text{hash}()$ としては、MD5 などがある。また、鍵 K としては、64 ビット鍵、 D C T_h a s h は 64 ビット長が妥当な長さである。

【0070】

[ハッシュ値埋込部 302]

ハッシュ値埋込部 302 は、ハッシュ値計算部 300 で選られた D C T_h a s h を画像に埋め込む。画像に埋め込むアルゴリズムは何を用いてもよいが、画像を痛めない方法としては L S B 法がよい。

L S B 法とは、電子透かしをデジタルコンテンツに埋め込む方式の 1 つで、コ

ンテンツの特徴量のLSB(least significant bit、最下位bit)をある規則に従って変化させることによって、情報を埋め込む。LSBを変化させる理由は、埋め込み後のデジタルコンテンツ（画像、音）の変化が殆ど無い為である。

【 0 0 7 1 】

以下、具体例を挙げて説明する。

埋込パラメータDB 2 0（図2）から得られる埋め込みに利用するDCT係数{d c t _ c o e f f i}の要素がn個あり、h a s h _ e m bが64ビットで、1つのサブブロック（8×8画素）にmビットを埋め込む事を考える(n>=m)。つまり、埋め込みに64/m個のサブブロックが必要となる。

【 0 0 7 2 】

ここで、埋め込みによる画質の痛みを極力防ぐ為に、Aの候補を予め幾つか決めておいて（例：画面の上、下、右、左端の4箇所）、そのどこかに埋めて、検出時に全て試すという方法もある。

さて、ここで、{d c t _ c o e f f i}のLSBに埋めたいb i tを埋めていくわけである。

【 0 0 7 3 】

【数 1 0】

$$\text{emb_coeff}[k] = 2p + \text{emb_bit}[k] \quad (10)$$

pはある整数、emb_bit[k]は係数kに埋めたいbit, 0 or 1

【 0 0 7 4 】

上式10を満たすようにemb__c o e f f [k]を変更後、Aの領域のみのDCT係数をJ P E G' /BMP変換部326（図5）に入力し、A内の全ての{d c t _ c o e f f i}のDCT係数が、上式10を満たしつつ安定になるようにすれば良い。

この場合、常に、emb_coeff[k]の値の絶対値が大きくなる方向に変更していれば、つまりαを小さく取れば、収束は速く、式6が達成できる。式6が達成出来れば、Aは安定の為、BMPデータに変換した後も、埋めたビットが変化しない。

【 0 0 7 5 】

〔出力フォーマット変換部 3 0 4〕

出力フォーマット変換部 3 0 4 は、ハッシュ値埋込部 3 0 2 の出力結果に対して量子化処理などを行い、入力装置 1 0 2（図 1）を介して設定されるユーザ所望の出力フォーマットに変換する。

出力フォーマットが J P E G の際、 $\{d c t_c o e f f i\}$ に属する D C T 係数も、 $q_e m b [k]$ ではなく、 $q [k]$ で量子化する。 $q [k]$ で量子化された値 $c o e f f [k]$ は、 $e m b_c o d f f [k]$ 、 $q [k]$ 、 $q_e m b [k]$ より、 $c o e f f [k] = e m b_c o e f f [k] * q_e m b [k] / q [k]$ によって計算される。

〔0 0 7 6〕

〔検出部 4 0〕

以下、検出部 4 0（図 2）を説明する。

埋め込み装置で埋め込まれた画像データを入力し、鍵 K より注目する D C T 成分のハッシュ値を計算し、領域 A に埋め込まれているハッシュ値と比較し、画像自体が改ざんされたかどうかを検出する。

〔0 0 7 7〕

〔検出前処理部 4 2〕

図 7 は、図 2 に示した検出部 4 0 の構成を示す図である。

図 8 は、図 7 に示した検出前処理部 4 2 の構成を示す図である。

検出部 4 0 において、検出前処理部 4 2 は、入力画像より埋め込み量子化値 $q_e m b [k]$ を逆算する。

〔0 0 7 8〕

〔フォーマット認識部 4 2 0〕

フォーマット認識部 4 2 0 は、入力画像のフォーマットを認識し、J P E G なら復号部 4 2 2 に対して出力し、B M P、Y U V なら B M P、Y U V / J P E G' 変換部 4 2 4 に対して出力する。

〔0 0 7 9〕

〔復号部 4 2 2〕

復号部 4 2 2 は、入力画像を復号し、A を除く画像全体の注目する D C T 成分の係数を逆量子化して、J P E G' 画像とする。

【 0 0 8 0 】

[BMP, YUV/JPEG' 変換部 4 2 4]

BMP, YUV/JPEG' 変換部 4 2 4 は、入力された BMP, YUV データを DCT 処理し、JPEG' データに変換する。

【 0 0 8 1 】

[量子化値逆算部 4 2 6]

【 0 0 8 2 】

図 9 および図 10 は、図 8 に示した量子化値逆算部 4 2 6 における埋め込み量子化値逆算処理を示す第 1 および第 2 のフローチャートである。

量子化値逆算部 4 2 6 は、復号部 4 2 2 および BMP, YUV/JPEG' 変換部 4 2 4 の出力の注目する DCT 成分 $k \in \{dct_coeff\}$ の画像全体での絶対値の最大係数を $max[k]$ として、各々の仮定した量子化値 i の回りにどのくらい DCT 係数が集まっているかのヒストグラムから示すように計算する。

図 9 に示すように、フォーマット認識部 4 2 0 への入力フォーマットが JPEG の場合、 $i = q[k] * n$ ($n = 1, 2, \dots$) に対してのみ調べれば良い。

【 0 0 8 3 】

図 9 に示した処理により求められたヒストグラム $[i]$ の最大値を与える i を、 max_i とおき、図 10 に示した処理にしたがって、 $q_emb[k]$ を決定する。

図 10 では、図 9 で $q_emb[k]$ が、 max_i の倍数であることから $q_emb[k]$ を求めている。

【 0 0 8 4 】

ここで、 T_thre は 1 より少し小さい値で、 $T_thre = 0.8$ 辺りが妥当である。ここで、 T_thre の値の精度等より図 9 および図 10 に示した処理によりうまく $q_emb[k]$ が求められない例外的な画像に関して、埋め込み処理の過程において、図 9 および図 10 に示した処理により、正しく $q_emb[k]$ が満たされるようなヒストグラムになるようにすればよい。

例えば、 $q_emb[k] * 2^n$ の周りに多く係数が集まってしまうような場合、画像全体のうち、痛みが少なそうなところで、 $q_emb[k] * 2^{n+1}$ に埋め込むようにすれば良い。

【0085】

[ハッシュ値抽出部400]

再び図7を参照する。

ハッシュ値抽出400は、埋め込み領域Aにおいて、埋込パラメータDB20からの埋め込みDCT成分 $\{dct_coeff_i\}$ の係数 $c[k]$ と、検出前処理部42によって計算された、埋め込み量子化値 $q_emb[k]$ より、以下の方法でLSBをしらべ、それらを並べて埋め込まれたハッシュ値 $embed_hash$ を計算する。

【0086】

【数11】

$$LSB = (int)((c[k] + \beta) / q_emb[k]) \bmod 2$$

$$\text{但し、} \beta = c[k] \geq 0 ? q_emb[k] / 2 : -q_emb[k] / 2 \quad (11)$$

【0087】

[ハッシュ値計算部402]

ハッシュ値計算部402は、A以外の領域に対して、 $\{dct_coeff_i\}$ の係数 $C[k]$ $q_emb[k]$ より、上記式6においてで $\alpha=0.5$ として、 $coeff_emb[k]$ を求め、上記式9により DCT_hash を計算する。

【0088】

[改ざん検出部404]

改ざん検出部404は、ハッシュ値抽出400およびハッシュ値計算部402から得られる DCT_hash 、 $embed_hash$ が、 $DCT_hash = embed_hash$ なら改ざんなし、それ以外の場合 ($DCT_hash \neq embed_hash$) には改ざん有りとして、表示装置100 (図1) 等に表示する。

【0089】

[全体動作]

図 1 1 は、埋込・検出プログラム 2（図 2）による埋め込み処理を示すフローチャートである。

図 1 2 は、埋込・検出プログラム 2（図 2）による検出処理を示すフローチャートである。

なお、図 1 1 および図 1 2 の各処理中の括弧内の番号は、その処理を行う埋込・検出プログラム 2 の構成部分（図 3，5，7，8）に付された符号を示す。

埋込・検出プログラム 2 の各構成部分は、図 1 1 に示すように埋め込み処理を行い、図 1 2 に示すように検出処理を行う。

【0090】

〔変形例〕

以下、本発明に係る埋め込み装置の変形例を説明する。

図 1 3 は、埋込・検出プログラム 2（図 2）において埋込部 3 0 の代わりに用いられる埋込部 5 0 の構成を示す図である。

図 1 4 は、図 1 3 に示した埋込前処理部 5 2 の構成を示す図である。

図 1 5 は、図 1 3 に示した改ざんマーク埋込部 5 4 の構成を示す図である。

【0091】

なお、埋込部 5 0 の構成部分の内、出力フォーマット変換部 5 0 2 は、埋込部 3 0（図 3）の出力フォーマット変換部 3 0 4 に同じであり、埋込前処理部 5 2 の構成部分の内、フォーマット認識部 5 2 0、復号部 5 2 2、BMP，YUV／JPEG' 変換部 5 2 4、量子化値変換部 5 2 6 および量子化値計算部 5 2 6 は、それぞれ埋込前処理 3 2（図 5）のフォーマット認識部 3 2 0、復号部 3 2 2、JPEG'／BMP 変換部 3 2 6、YUV／BMP 変換部 3 2 8 および埋込量子化値計算部 3 2 4 に同じである。

また、埋込部 5 0 においては領域 A は存在しない。

【0092】

〔埋め込み前処理部 5 2〕

埋込前処理部 5 2 は、入力画像より、DCT 係数を抽出する。

【0093】

〔改ざんマーク埋め込み部 5 4〕

改ざんマーク埋込部 5 4 は、改ざんマークあるいはデータを埋め込む部分で、埋め込みアルゴリズムは何でも良く、画像を痛めない方法としては L S B 法がある。

【 0 0 9 4 】

[画像分割部 5 4 0]

画像を 8×8 画素のブロック（イントラブロック）単位に分割し、入力注目 DC T 成分 l , 係数 $c[k]$ と画像位置 (x, y) を出力する。

【 0 0 9 5 】

[乱数発生部 5 4 2]

乱数発生部 5 4 2 は、鍵 K より乱数 R を発生させる。 R は、埋め込みに必要な bit 数だけの bit が必要で、 720×480 画素の場合、 $90 \times 60 \times n = 5400n$ bit 以上である必要がある。 R の作成方法は色々あるが、 LFSR を使う場合、 $b = (\text{int})(1 + \log_2 5400n)$ bit の LFSR を使って、 K を key, R_0 を鍵 DB より得られる初期値（鍵の 1 部と考えるも良い）、 LFSR b を b bit の LFSR 計算部として、下式 1 2 により求められる。

【数 1 2】

$$R = \text{LFSR}_b(K, R_0) \quad (1\ 2)$$

【 0 0 9 6 】

[合成部 5 4 4]

合成部 5 4 4 は、データを埋め込む場合に、埋め込みデータと R より埋め込み bit 列 R' を合成して作成する。なお、合成部 5 4 4 が、改ざんマークを埋め込む場合、 $R' = R$ となる。データを埋め込む場合は、下式 1 3 により示される R' が埋め込み bit になる。ここで、 \wedge は xor を意味する。但し、 data は $5400n$ bit の埋め込み data で、埋め込みたい data が m bit で、 $m < 5400n$ bit の場合、埋め込み data を m 周期で繰り返し、 $5400n/m$ 回繰り返し埋める、等の方法もある。

【 0 0 9 7 】

【数 1 3】

$$R' = R \wedge \text{data} \quad (1\ 3)$$

【 0 0 9 8 】

[L S B 操作部 5 4 6]

LSB操作部546は、 R' と $q_emb[k]$, $c[k]$, k , (x, y) より、 $\{dct_coeffi\}$ に属するDCT係数のLSBを操作する。先ず、埋め込みビット $emb_bit[k]$ は、下式14を埋め、あとは、上記式10を満たすように、 $\{dct_coeffi\}$ に属する全てのDCT係数を $T[x][y] = 0$ を満たす全てのMCUに対して行う。

【0099】

【数14】

$$emb_bit[k] = (R' \gg (xn + 90yn + 1)) \& 1 \quad (14)$$

【0100】

【DCT成分分割部528】

DCT成分分割部528は、復号部522およびBMP、YUV/JPEG'変換部524から入力されるDCT係数(量子化されていない)を注目DCT($\{dct_coeffi\}$)とそうでないものに分ける。

【0101】

【量子化値計算部526】

量子化値計算部526は、上述したように埋込量子化値計算部324と同じである。但し、 $T[45][60]$ を、初期状態 ($T[x][y] = 0$ 、for all x, y) で出力する。

【0102】

図16は、図15に示した埋込後処理部56の構成を示す図である。

なお、埋込後処理部56の構成部分の内、DCT係数調整564は、埋込前処理32のDCT係数調整部332(図5)と同じである。

【0103】

【JPEG' / BMP変換部560】

JPEG' / BMP変換部560は、入力されたJPEG' 画像をiDCT変換して、オーバーフロー/アンダーフロー処理をして、BMPフォーマットの画像に変換する。

【0104】

【BMP / JPEG' 変換部562】

BMP/JPEG' 変換部 6 0 0 は、入力 BMP 画像を DCT 変換し、JPEG' フォーマットの画像に変換する。

【 0 1 0 5 】

図 1 7 は、埋込・検出プログラム 2 (図 2) において、検出部 4 0 の代わりに用いられる検出部 6 0 の構成を示す図である。

検出部 6 0 は、図 1 3 ~ 1 6 に示した検出部 4 0 により埋め込まれた画像データが、データ埋め込みでなく、改ざんマークを埋め込みである場合、その画像の改ざんの有無を検出し、改ざん場所を 8×8 画素のブロック単位で特定する。

$\{dct_coeff_i\}$ の要素が n 個ある場合、各々の 8×6 画素構成のブロック (イントラブロック) の改ざん検出率は $1-2^{-n}$ であり、本発明例の様に $n=4$ の場合、その確率は 93.75% である。

【 0 1 0 6 】

[検出前処理部 6 0 0]

検出前処理部 6 0 0 は、図 7 に示した検出前処理部 4 2 と同じである。但し、埋込領域 A はない。

【 0 1 0 7 】

[埋め込みデータ抽出部 6 0 2]

埋込データ抽出部 6 0 2 は、 $\{dct_coeff_i\}$ の要素の DCT 係数の LSB を抽出し、埋め込みデータを抽出する。

イントラロケーション (x, y) ($0 \leq x < 60, 0 \leq y < 90$), $\{dct_coeff_i\}$ の要素数 n の LSB を式 1 1 により計算し、それを $(xn+90yn+1)$ bit 目に持つ $5400n$ bit の抽出データ $embed_data$ を計算する。

【 0 1 0 8 】

[埋め込みデータ計算部 6 0 4]

埋込データ計算部 6 0 4 は、図 1 5 に示した乱数発生部 5 4 2 および合成部 5 4 4 と同じ方法で、埋め込み bit 列 R' を計算する。

【 0 1 0 9 】

[改ざん検出・場所特定部 6 0 6]

改ざん検出場所特定部 6 0 6 は、 $embed_data$, R' から入力画像に

改ざんがあったかどうか、あった場合、何処が改ざんされたかを特定する。つまり、改ざん検出場所特定部 6 0 6 は、 $embed_data == R'$ の場合、改ざんなしと判定し、これ以外の場合 ($embed_data <> R'$) には、ビット単位で値が合わない部分を全て探す。その際、例えば、 p bit 目 (0 origin) が合わない場合、改ざんのあった intra location (x,y) は、以下の式によって特定出来る。

【0 1 1 0】

【数 1 5】

$x = (int)(p/n) \bmod 90$

$y = (int)(p/n/90)$ (1 5)

【0 1 1 1】

【出力フォーマット変換部 6 0 8】

出力フォーマット変換部 6 0 8 は、画像 DB 2 4 より入力した画像を、改ざん場所がわかるように変化させて出力する。

【0 1 1 2】

【全体動作】

図 1 8 および図 1 9 は、検出部 4 0 および検出部 6 0 の処理を示すフローチャートであり、図中の括弧内の番号は、各処理を行う構成部分の符号を示す。

検出部 4 0 および検出部 6 0 は、図 1 8 に示すように埋め込み処理を行い、図 1 9 に示すように検出処理を行う。

【0 1 1 3】

【発明の効果】

上述したように、本発明にかかる画像処理装置およびその方法は、圧縮符号化に適している。

特定的には、本発明にかかる画像処理装置およびその方法によれば、認証情報を埋め込んだ後に量子化処理をしても、埋め込まれた認証情報が失われることがない。

【図面の簡単な説明】

【図 1】

本発明にかかる画像処理方法を実現する画像処理装置の構成を示す図である。

【図 2】

図 1 に示した画像処理装置が実行し、本発明にかかる画像処理方法を実現する埋込・検出プログラムの構成を示す図である。

【図 3】

図 2 に示した埋込部の構成を示す図である。

【図 4】

注目 DCT 係数を示す図である。

【図 5】

図 3 に示した埋込前処理部の構成を示す図である。

【図 6】

(A) は、図 3 に示した埋込前処理による安定化処理の前の注目 DCT 係数 dct_coeff_i の値の頻度を $q[k] = 3$, $q_emb[k]$ の場合について例示し、(B) は埋込前処理による安定化処理の後の注目 DCT 係数 dct_coeff_i の値の頻度を同様に例示するヒストグラムである。

【図 7】

図 2 に示した検出部の構成を示す図である。

【図 8】

図 7 に示した検出前処理部の構成を示す図である。

【図 9】

図 8 に示した量子化値逆算部における処理を示す第 1 のフローチャートである。

【図 10】

図 8 に示した量子化値逆算部における処理を示す第 2 のフローチャートである。

【図 11】

埋込・検出プログラム（図 2）による埋め込み処理を示すフローチャートである。

【図 12】

埋込・検出プログラム（図 2）による検出処理を示すフローチャートである。

【図 1 3】

埋込・検出プログラム（図 2）において埋込部の代わりに用いられる埋込部の構成を示す図である。

【図 1 4】

図 1 3 に示した埋込前処理部の構成を示す図である。

【図 1 5】

図 1 3 に示した改ざんマーク埋込部の構成を示す図である。

【図 1 6】

図 1 5 に示した埋込後処理部の構成を示す図である。

【図 1 7】

埋込・検出プログラム（図 2）において用いられる第 2 の検出部の構成を示す図である。

【図 1 8】

検出部および検出部（図 1 3 ～ 1 7）の処理を示す第 1 のフローチャートである。

【図 1 9】

検出部および検出部（図 1 3 ～ 1 7）の処理を示す第 2 のフローチャートである。

【符号の説明】

1 . . . 画像処理装置

1 0 0 . . . 表示装置

1 0 2 . . . 入力装置

1 0 4 . . . カメラ I F

1 0 6 . . . メモリカード I F

1 0 8 . . . 記憶装置

1 1 0 . . . P C 本体

1 1 2 . . . メモリ

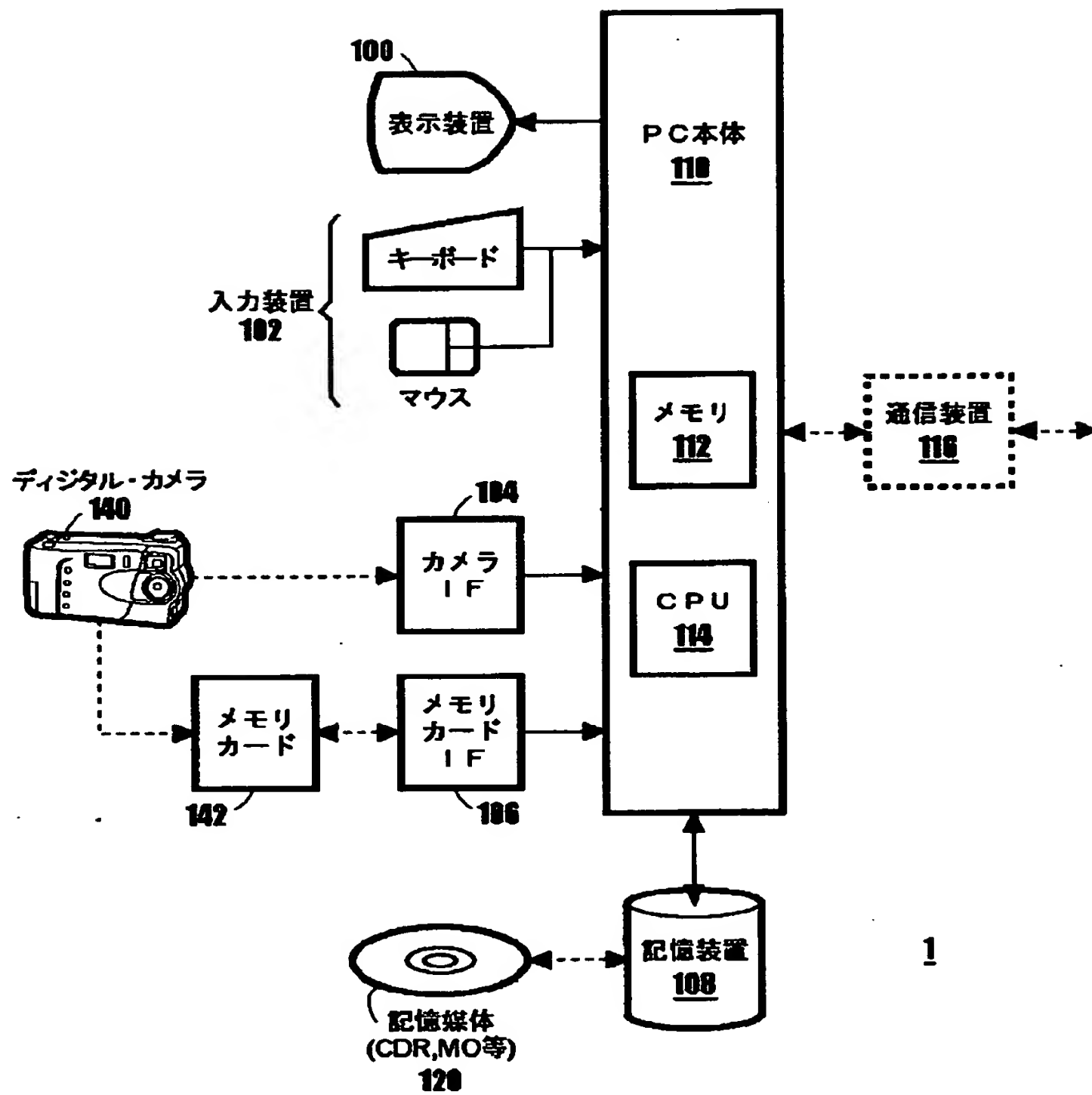
1 1 4 . . . C P U

- 1 1 6 . . . 通信装置
- 1 2 0 . . . 記録媒体
- 1 4 0 . . . デジタルカメラ
- 1 4 2 . . . メモリカード
- 2 . . . 埋込・検出プログラム
 - 2 0 . . . 埋込パラメータ D B
 - 2 2 . . . 鍵情報 D B
 - 2 4 . . . 画像 D B
 - 2 6 . . . 制御部
 - 3 0 . . . 埋込部
 - 3 2 . . . 埋込前処理
 - 3 2 0 . . . フォーマット認識部
 - 3 2 2 . . . 復号部
 - 3 2 4 . . . 埋込量子化値計算部
 - 3 2 6 . . . J P E G ' / B M P 変換部
 - 3 2 8 . . . Y U V / B M P 変換部
 - 3 3 0 . . . B M P / J P E G ' 変換部
 - 3 3 2 . . . D C T 係数調整部
 - 3 0 0 . . . ハッシュ値計算部
 - 3 0 2 . . . ハッシュ値埋込部
 - 3 0 4 . . . 出力フォーマット変換部
 - 4 0 . . . 検出部
 - 4 2 . . . 検出前処理部
 - 4 2 0 . . . フォーマット認識部
 - 4 2 2 . . . 復号部
 - 4 2 4 . . . B M P , Y U V / J P E G ' 変換部
 - 4 2 6 . . . 量子化値逆算部
 - 4 0 0 . . . ハッシュ値抽出
 - 4 0 2 . . . ハッシュ値計算部

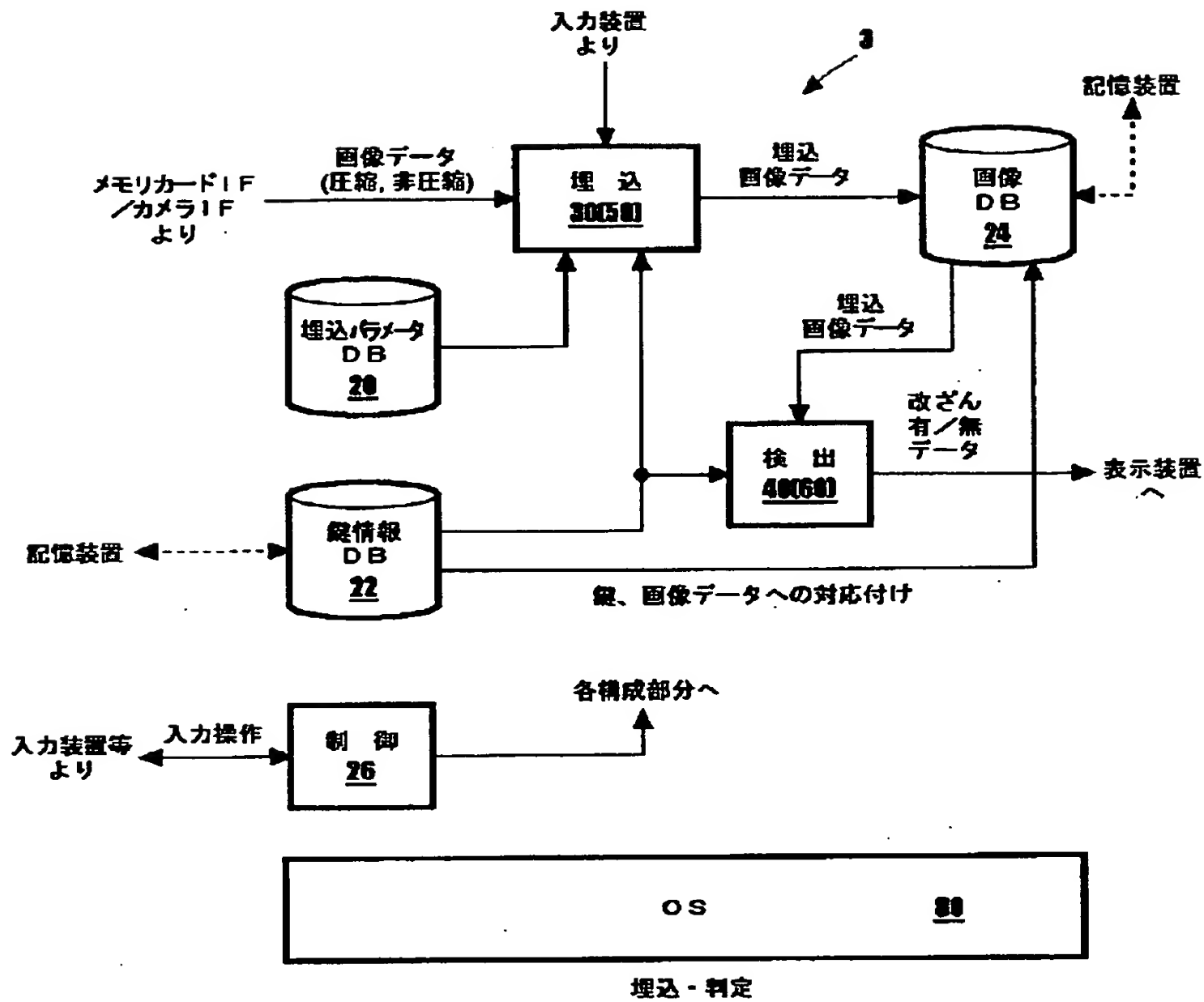
- 4 0 4 . . . 改ざん検出部
- 5 0 . . . 埋込部
 - 5 2 . . . 埋込前処理部
 - 5 2 0 . . . フォーマット認識部
 - 5 2 2 . . . 復号部
 - 5 2 4 . . . BMP, YUV / JPEG' 変換部
 - 5 2 6 . . . 量子化値計算部
 - 5 2 8 . . . DCT成分分割部
 - 5 4 . . . 改ざんマーク埋込部
 - 5 4 0 . . . 画像分割部
 - 5 4 2 . . . 乱数発生部
 - 5 4 4 . . . 合成部
 - 5 4 6 . . . LSB操作部
 - 5 6 . . . 埋込後処理部
 - 5 6 0 . . . JPEG' / BMP変換部
 - 5 6 2 . . . BMP / JPEG' 変換部
 - 5 6 4 . . . DCT係数調整部
- 5 0 2 . . . 出力フォーマット変換部
- 6 0 . . . 検出部
 - 6 0 0 . . . 検出前処理部
 - 6 0 2 . . . 埋込データ抽出部
 - 6 0 4 . . . 埋込データ計算部
 - 6 0 6 . . . 改ざん検出場所特定部
 - 6 0 8 . . . 出力フォーマット変換部
- 8 0 . . . OS

【書類名】 図面

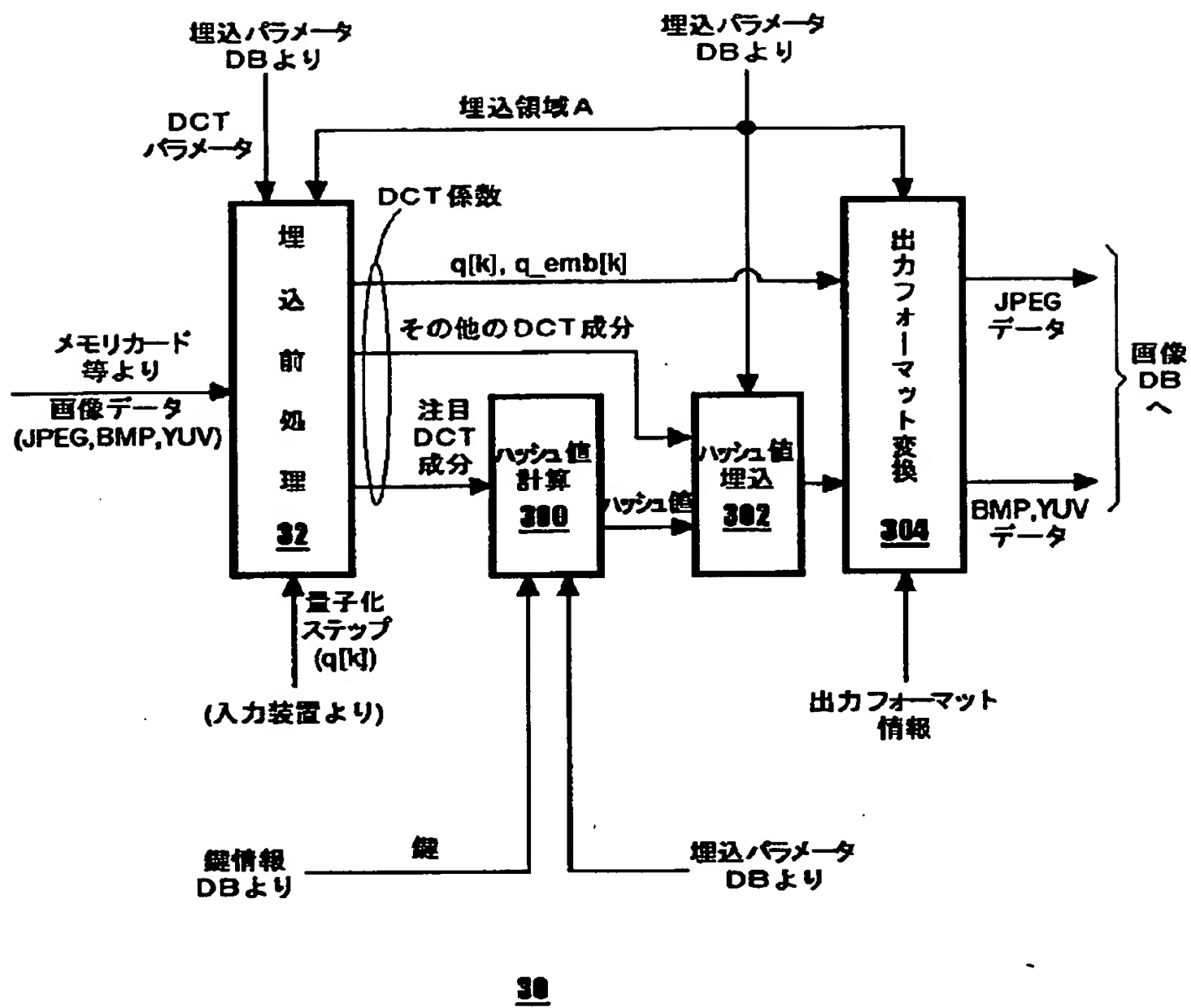
【図 1】



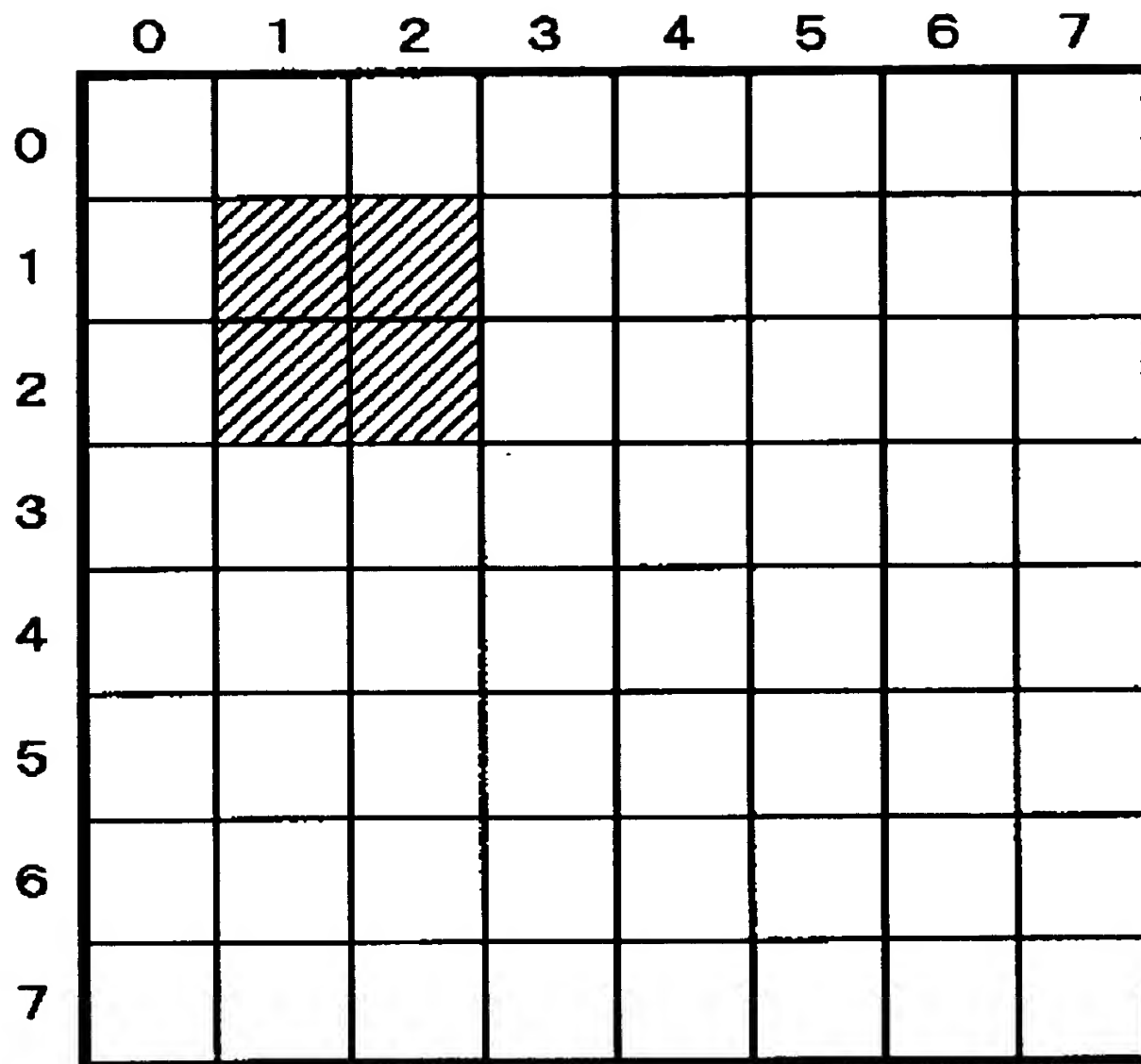
【図 2】



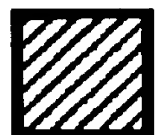
【図 3】



【図 4】

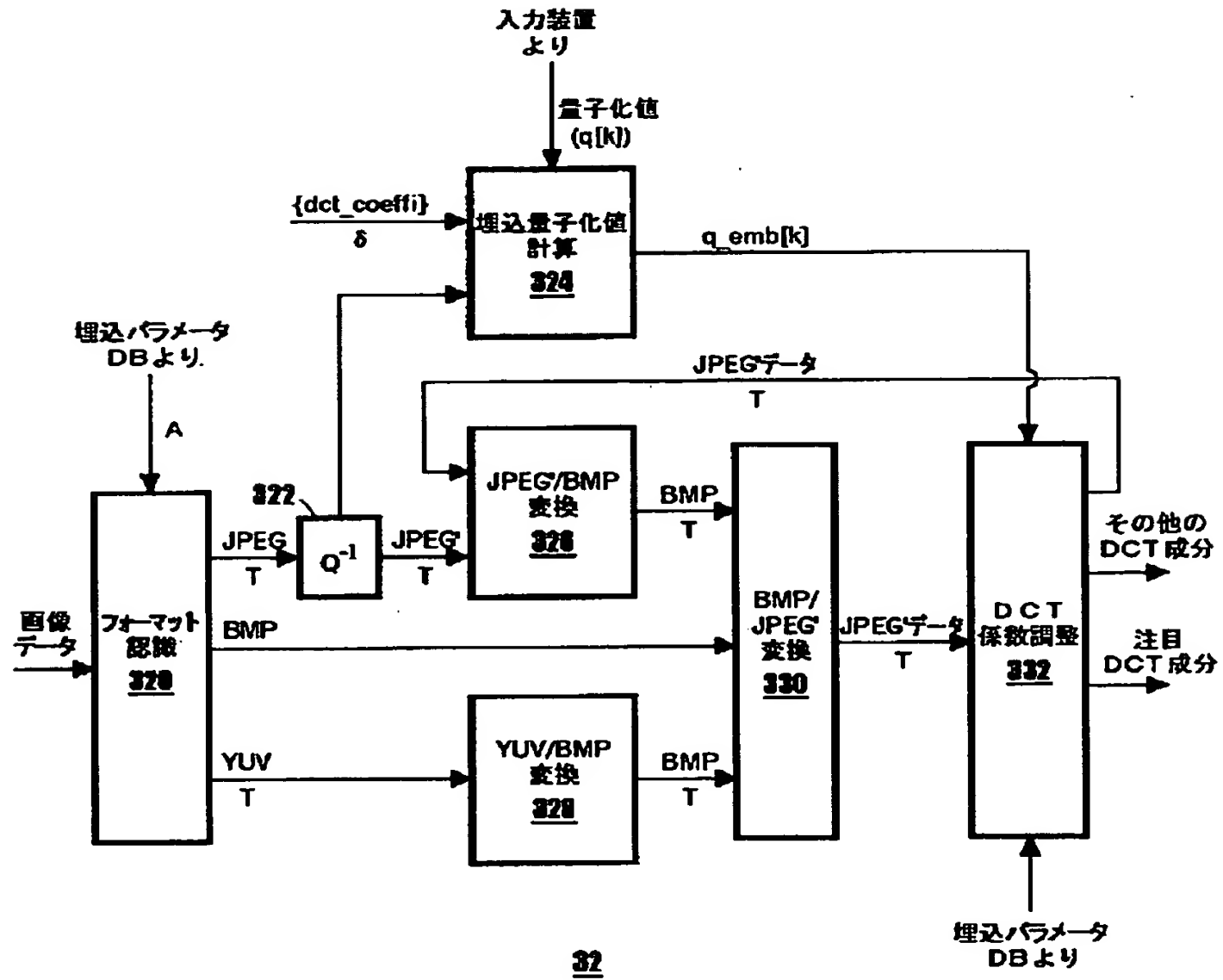


Y 成分 DCT 係数

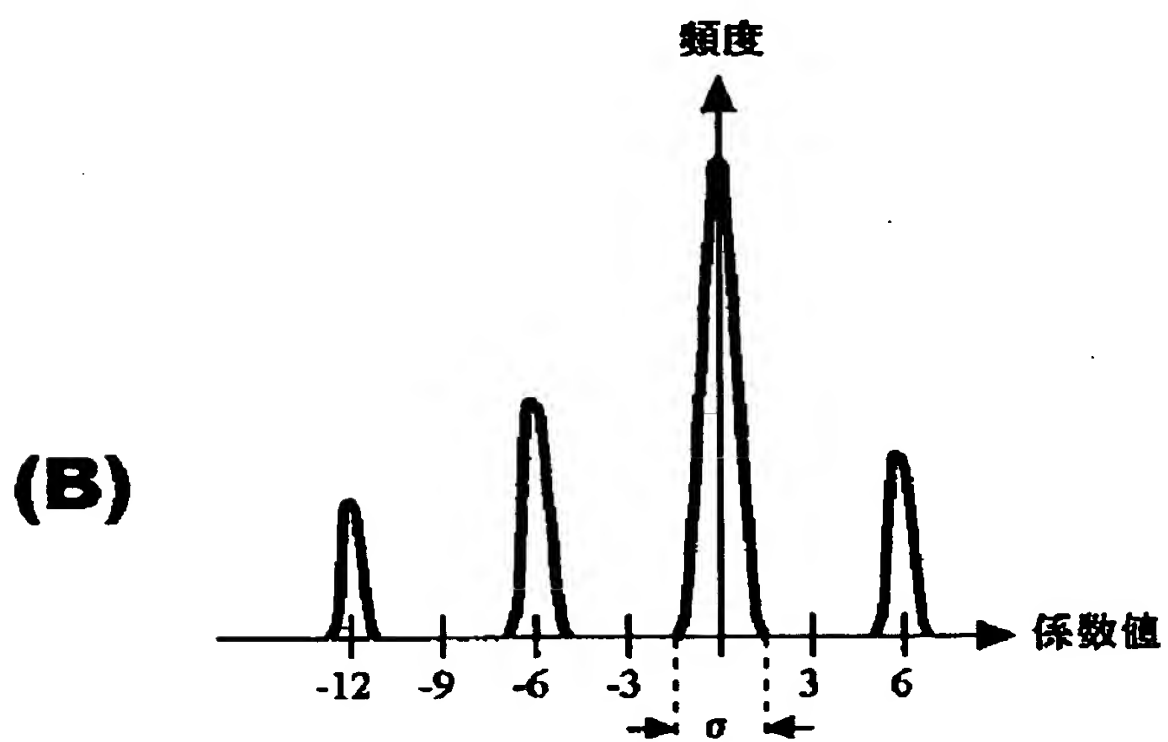
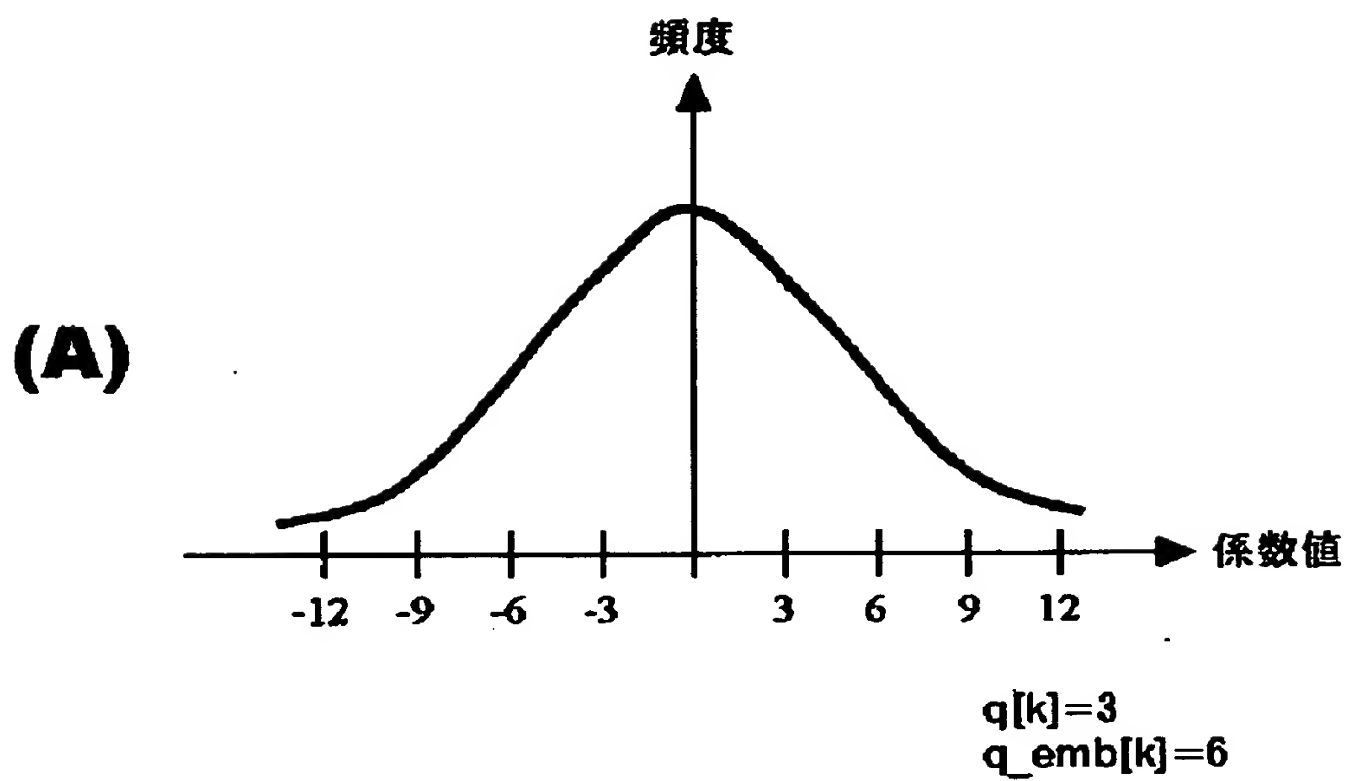


注目する DCT 成分

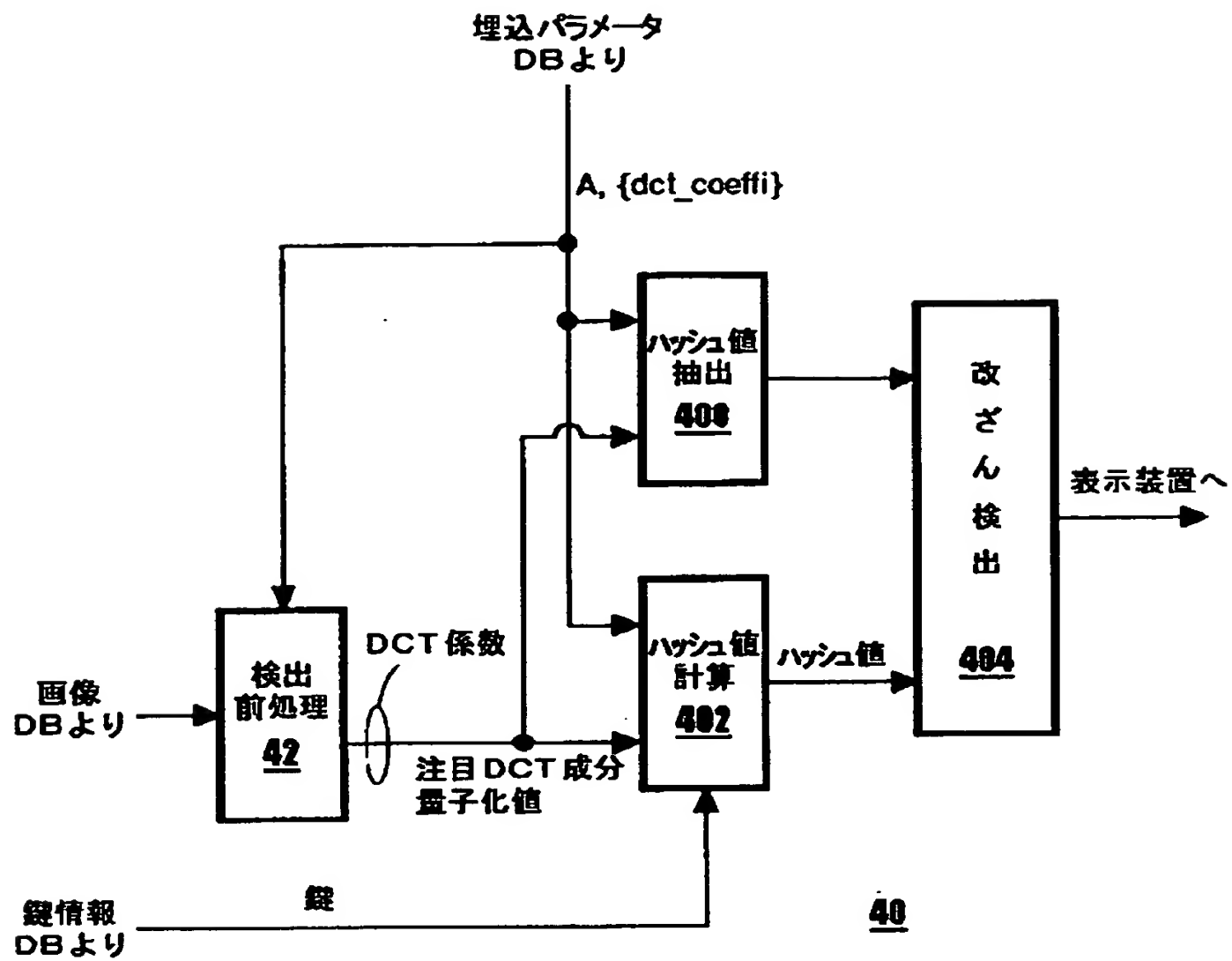
【図 5】



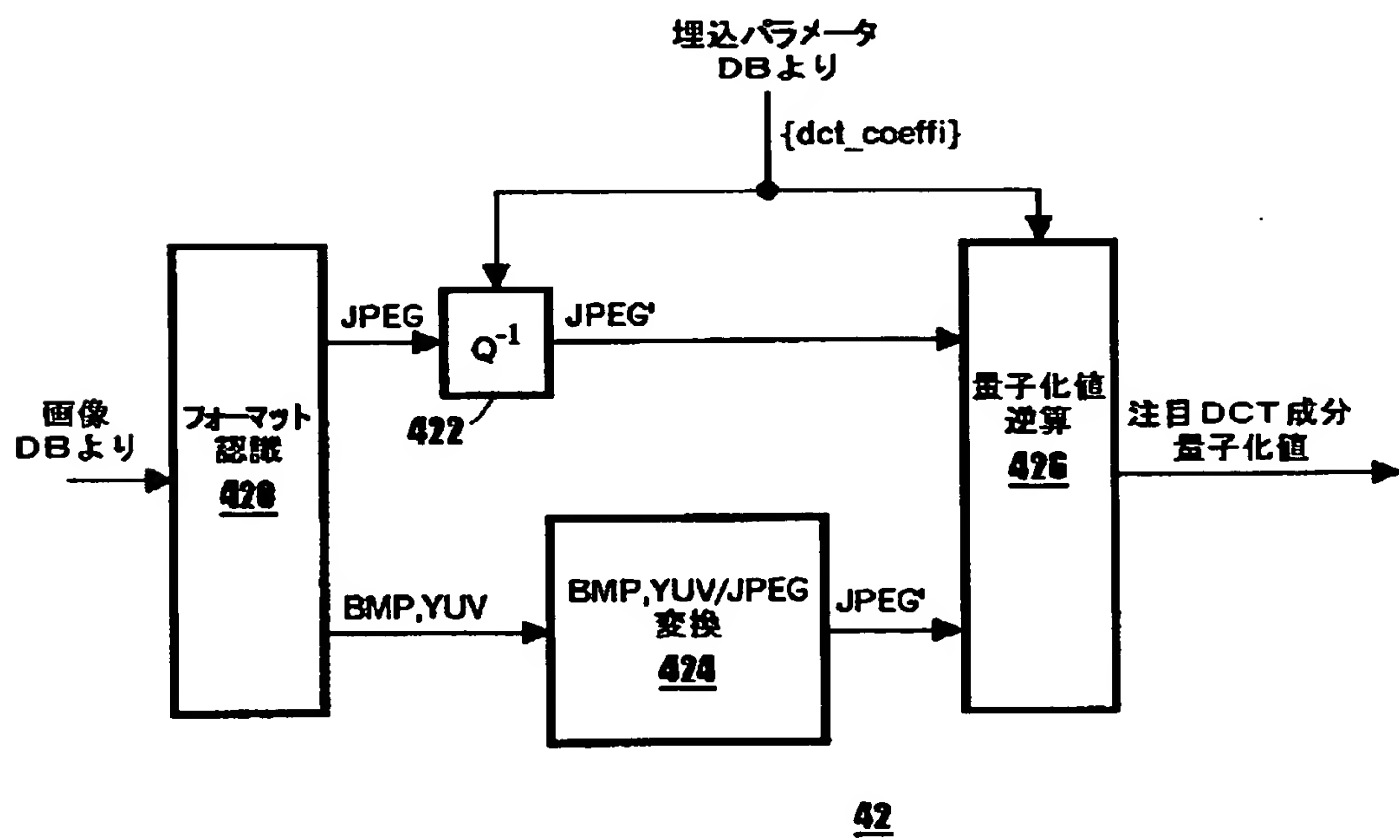
【図 6】



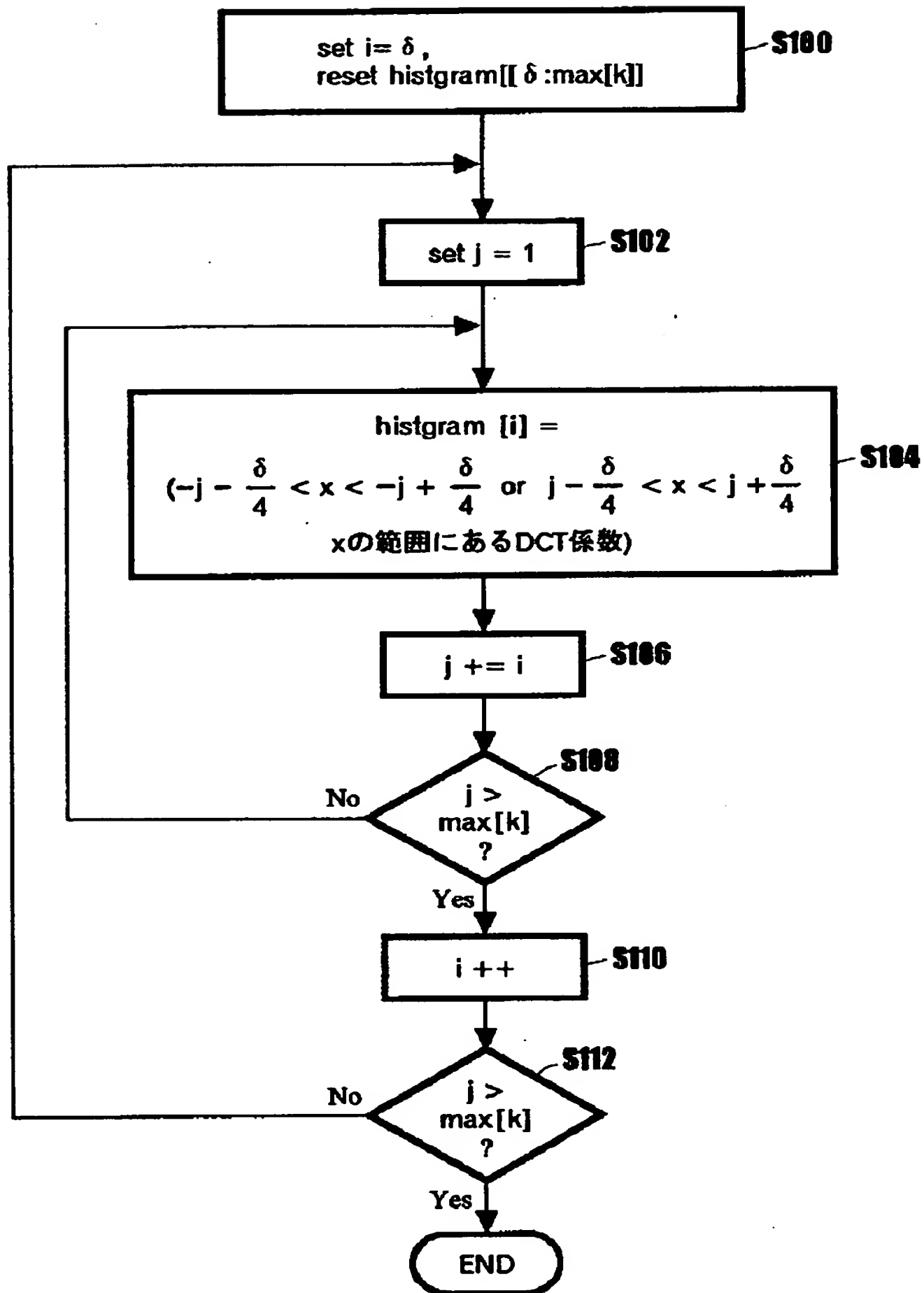
【図 7】



【図 8】

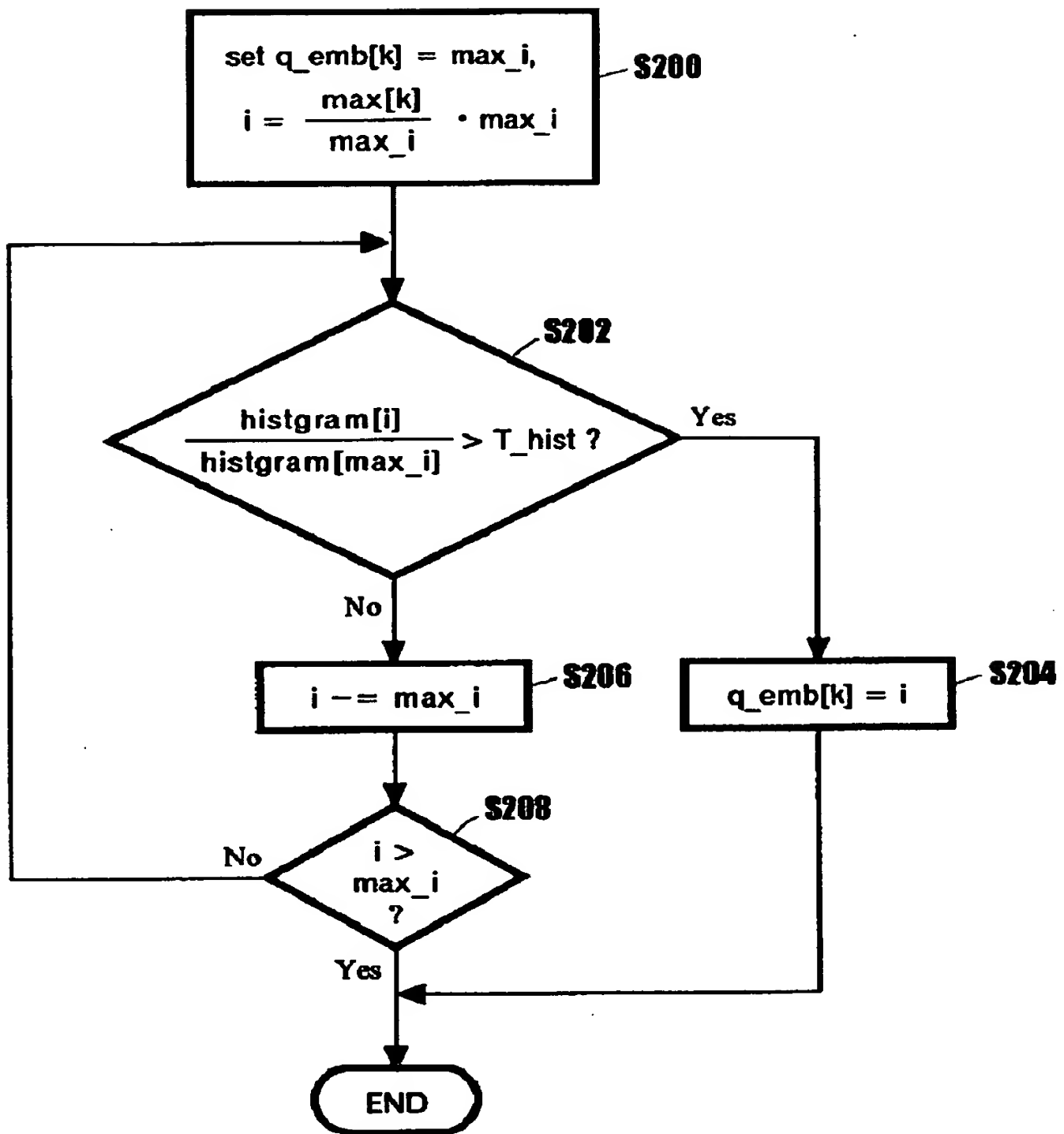


【図 9】



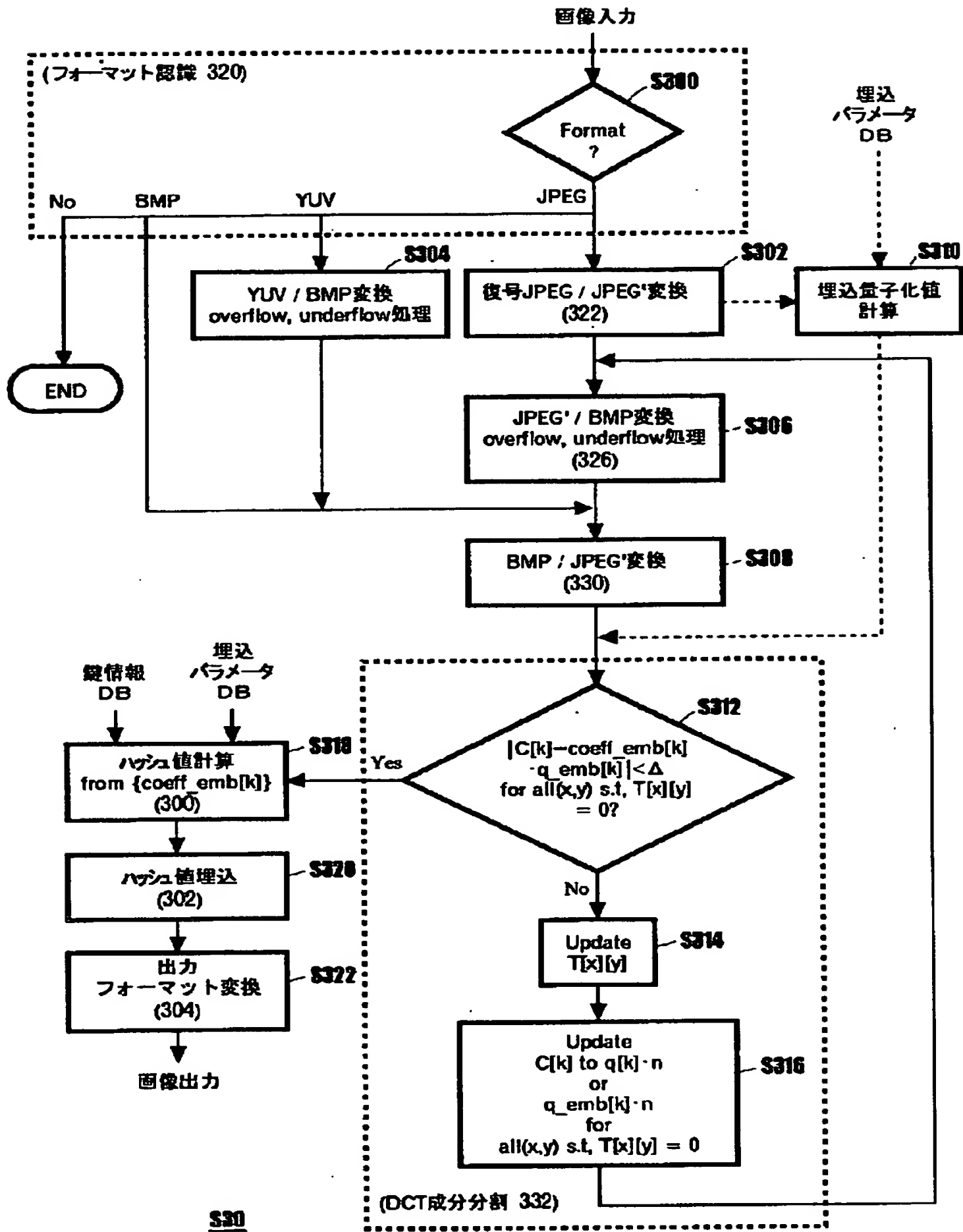
S10

【図 10】

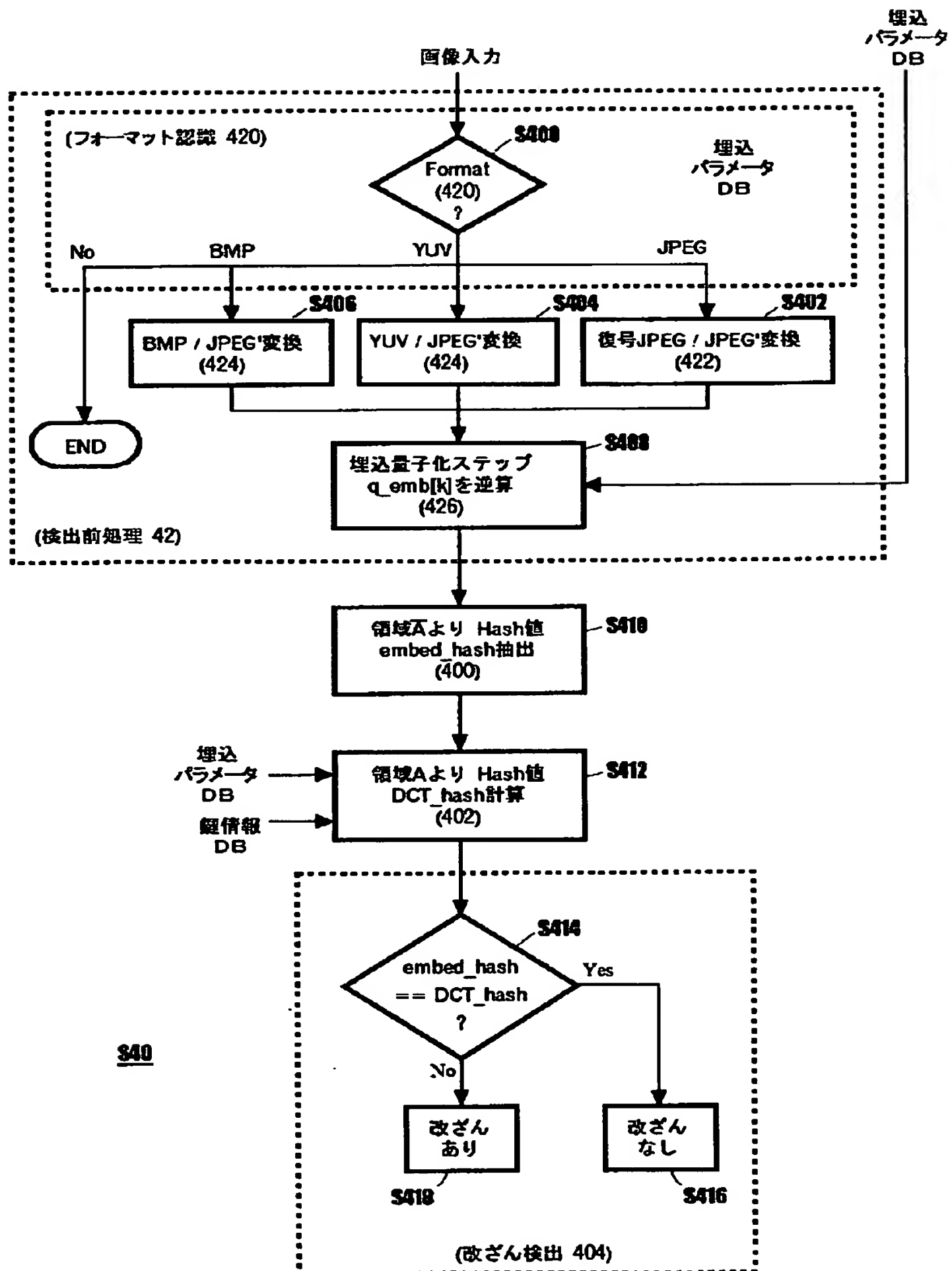


S20

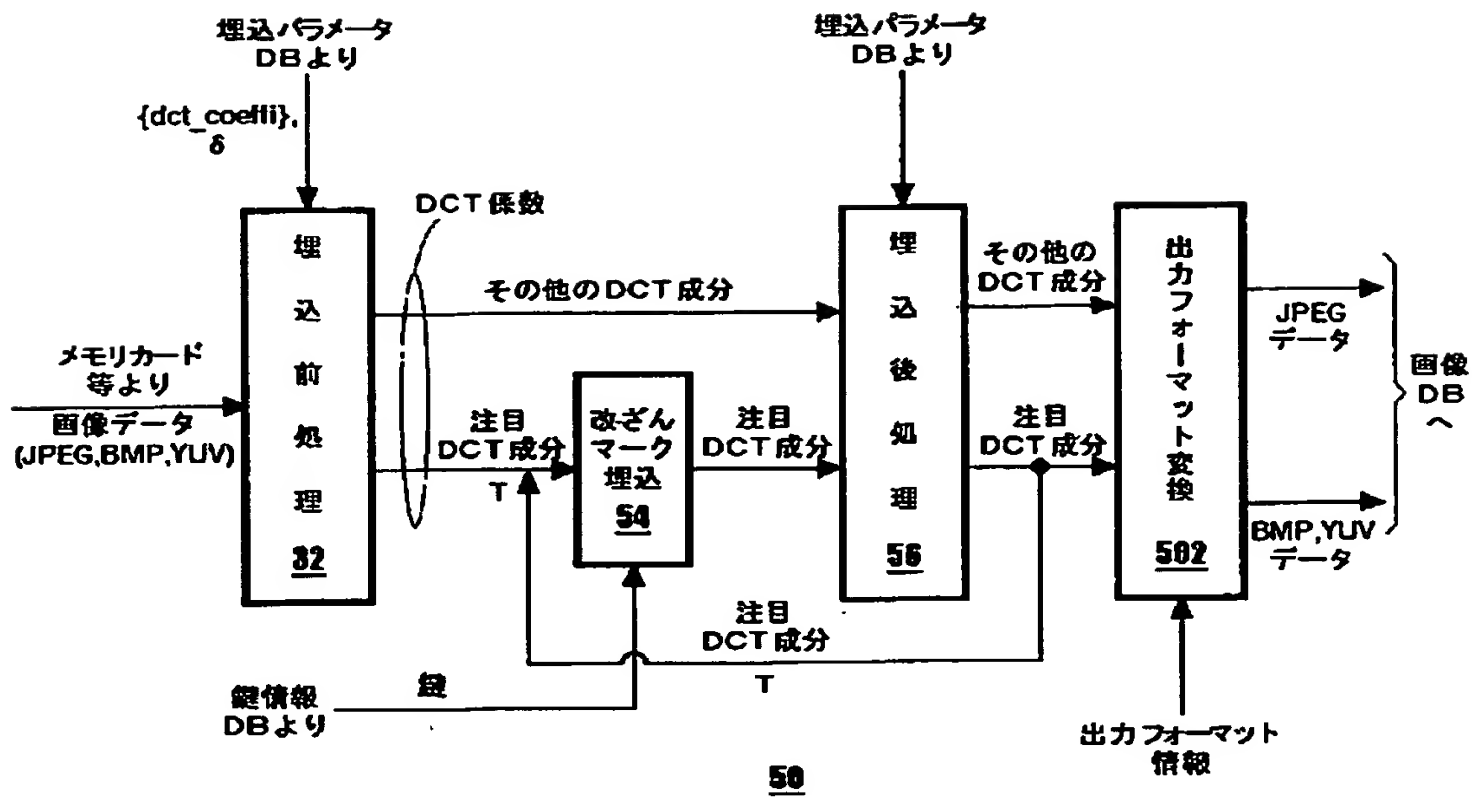
【図11】



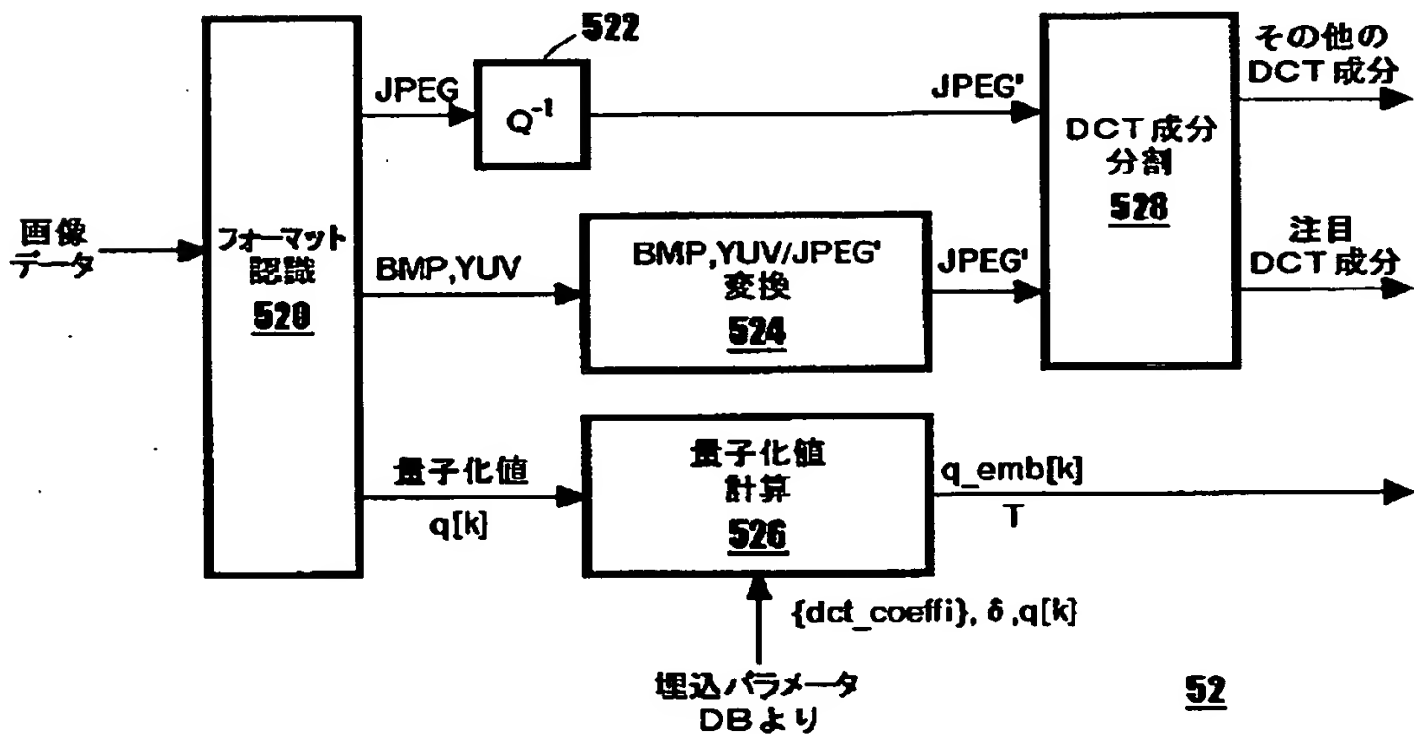
【図 1 2】



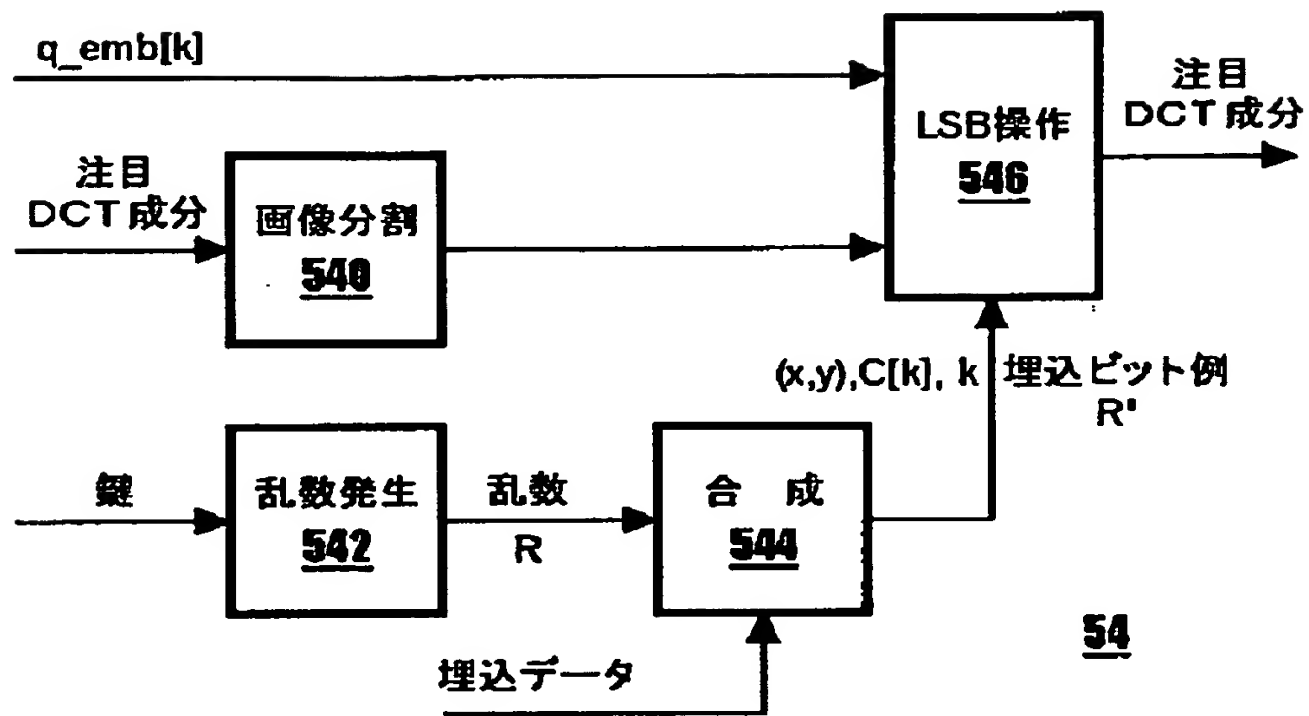
【図 1 3】



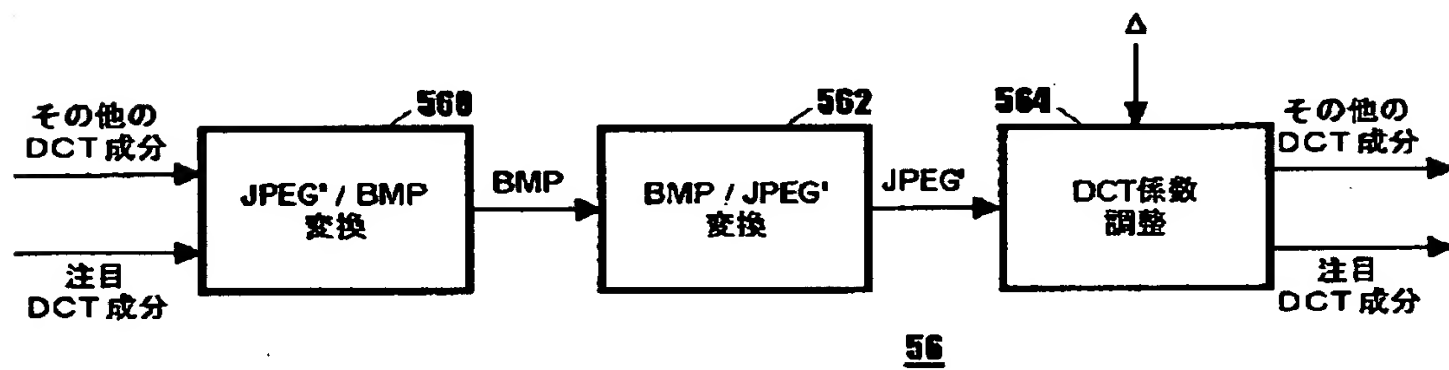
【図 1 4】



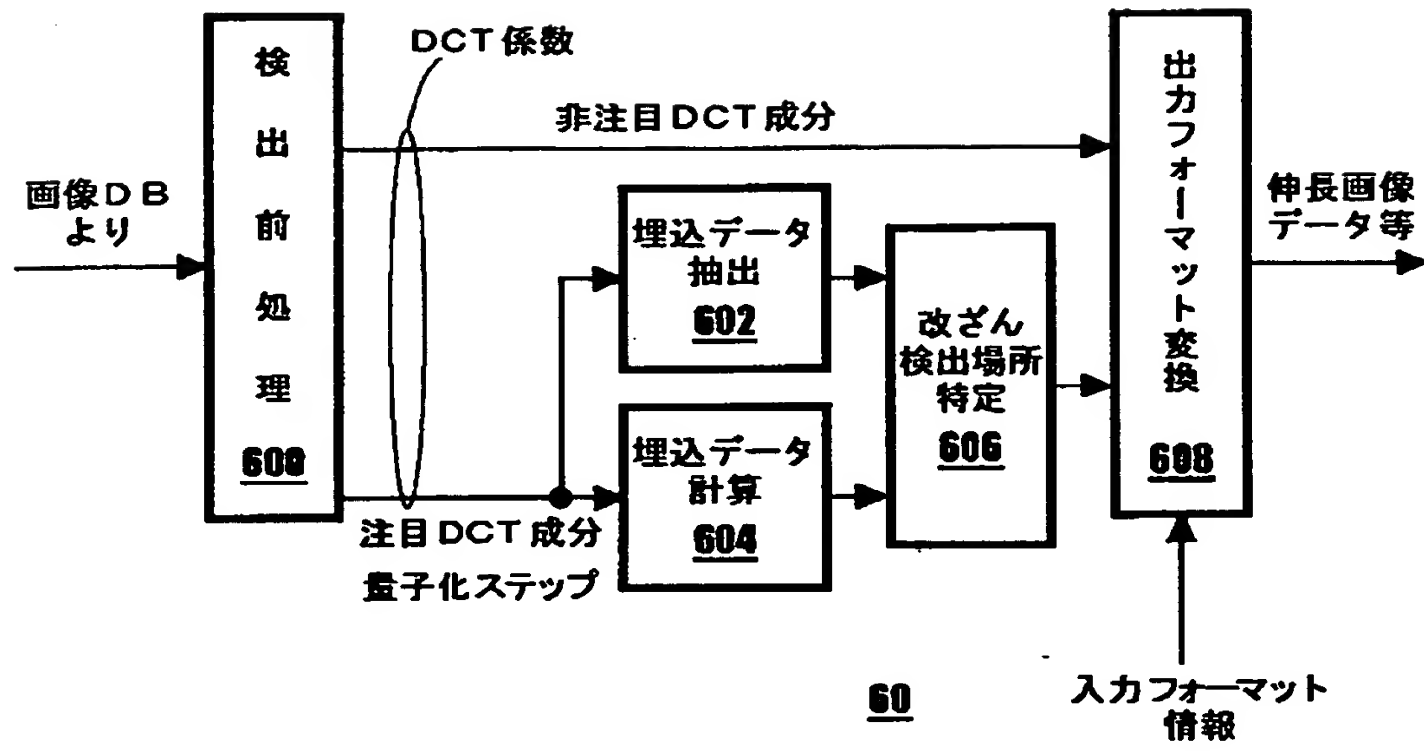
【図 1 5】



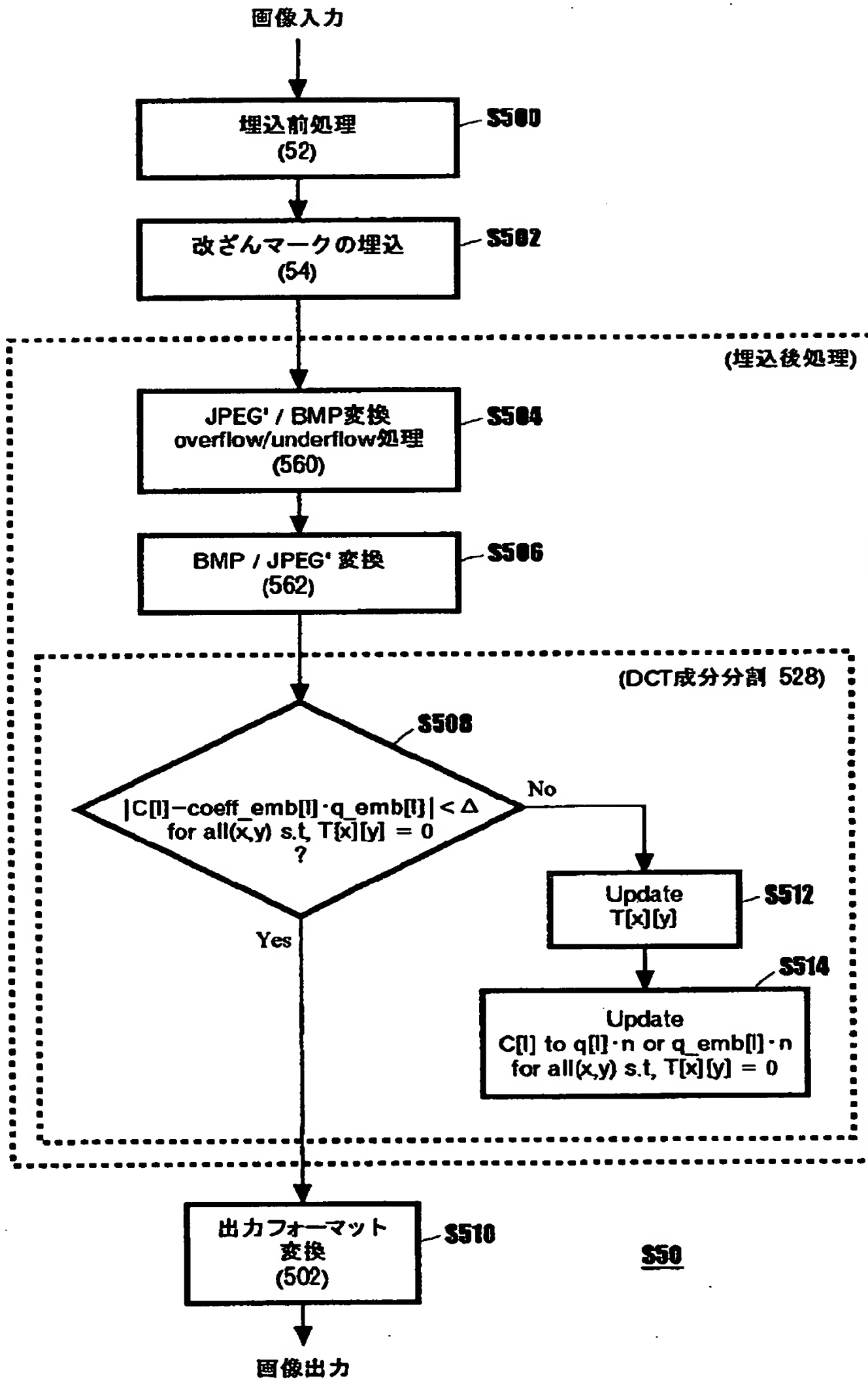
【図 1 6】



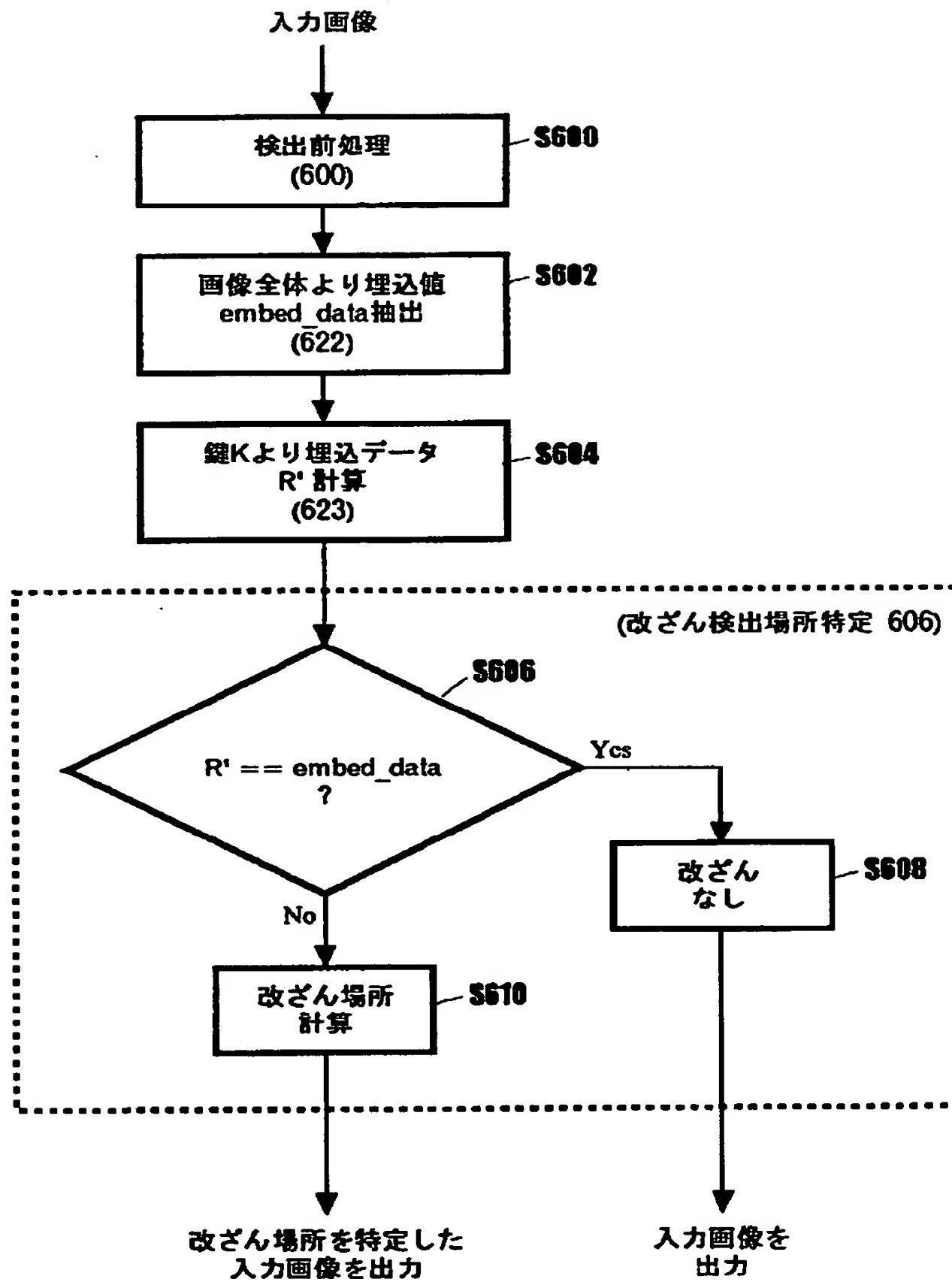
【図 17】



【図 18】



【図19】



S60

【書類名】 要約書

【要約】

【課題】 認証情報を埋め込んだ後に量子化処理をしても、埋め込まれた認証情報が失われることがないようにする。

【解決手段】 埋込前処理部 3 2 は、埋め込みデータの埋め込み処理により加わる誤差によって量子化処理後の値が変化しないように画像データの値を変換する。ハッシュ値計算部 3 0 0 は、画像データと鍵情報からハッシュ値を計算し、ハッシュ値埋込部 3 0 2 は、画像データにハッシュ値を埋め込む。出力フォーマット変換部 3 0 4 は、ハッシュ値が埋め込まれた画像データを量子化処理などし、J P E G データを生成する。

【選択図】 図 3

認定・付加情報

特許出願の番号	特願2000-012520
受付番号	50000058362
書類名	特許願
担当官	第七担当上席 0096
作成日	平成12年 1月24日

<認定情報・付加情報>
【提出日】

平成12年 1月21日

出 願 人 履 歴 情 報

識別番号 [390009531]

1. 変更年月日 1990年10月24日

[変更理由] 新規登録

住 所 アメリカ合衆国10504、ニューヨーク州 アーモンク (番地なし)

氏 名 インターナショナル・ビジネス・マシーンズ・コーポレイション